COMMUTATION ALGEBRAS OF GROUPS

by

NARAIN DATT GUPTA

M.A., LL.B. (Aligarh)

A thesis presented to the
Australian National University
for the degree of
Doctor of Philosophy
in the
Department of Mathematics
Institute of Advanced Studies

Canberra
1965

549848

STATEMENT

The only results which are not mine and which have been used in this thesis are stated with references in Chapter I. Some joint investigations and some work depending upon these joint investigations were also done but they do not form a part of the present thesis (see [8], [9] and [10]).

(N.D. Gupta)

PREFACE

This work was done while I received generous financial assistance from the Australian National University in the form of a research scholarship from April 1963 till now.

I am greatly indebted to my supervisor Professor B.H. Neumann, F.A.A.,F.R.S., and express my sincerest thanks to him for suggesting the study of Commutation Algebras and for his general guidance.

I also thank Dr L.G. Kovács who acted as my supervisor during the temporary absence of Professor Neumann.

The contents of Chapter IV and most of the contents of Chapter II are contained in my paper [5]. The contents of Chapter V are to appear in [6] and Chapter VI forms a part of my paper [7] . The results of Chapter III will be submitted for publication in the near future.

Other work which I have done but which has not been recorded in this thesis, is contained in [10] (with M.F. Newman), [9] (with H. Heineken) and [8] (independently)

The stencils for this thesis were cut by Mrs A. Debnam to whom I offer my thanks.

(N.D. Gupta)

TABLE OF CONTENTS

LIST OF NOTATIONS

$\lvert S \rvert$	the cardinal of the set S
$gp\{a,b,\ldots\}$	the group generated by $a,b,\ldots$
a^b	$b^{-1}ab$
$[a,b]$	the commutator of a and b (i.e. $a^{-1}b^{-1}ab$)
$\rho(a)$	the mapping which takes every element g of a group G to $[g,a]$
$\lambda(a)$	the mapping which takes every element g of a group G to $[a,g]$.
$P(G)$	the semigroup generated by all mappings $\rho(a)$
$\Lambda(G)$	the semigroup generated by all mappings $\lambda(a)$
$\underline{\underline{M}}(G)$	the near-ring generated by all mappings $\rho(a)$ and $\lambda(a)$.
$\underline{\underline{R}}(G)$	the algebraic system generated by all mappings $\rho(a)$ only
$\underline{\underline{L}}(G)$	the algebraic system generated by all mappings $\lambda(a)$ only
$Z(G)$	the centre of G .

$C(G)$	the centralizer of G
G'	the derived group of G
$\gamma_i(G)$	the ith term of the lower central series of G
ϕ	the empty set
$\mathrm{ind}_m n$	the least positive solution x of the congruence $n^x \equiv 1 \pmod{m}$
$\mathrm{ind}_m^* n$	the least positive solution x of the congruence $n^x \equiv -1 \pmod{m}$

INTRODUCTION

Let G be a group and let $\Omega(G)$ denote the semigroup of all mappings of G into G with the usual composition of mappings as multiplication, namely $g(\theta_1\theta_2) = (g\theta_1)\theta_2$.

With each element $x \in G$ we associate two mappings $\rho(x)$ and $\lambda(x)$ of G into G defined as follows:

$$\rho(x) : g \longrightarrow g^{-1}x^{-1}gx \ , \quad \lambda(x) : g \longrightarrow x^{-1}g^{-1}xg \ .$$

Let $P(G)$ denote the subsemigroup of $\Omega(G)$ generated by all ρ's and let $\Lambda(G)$ denote the corresponding subsemigroup generated by all λ's. These semigroups will be called the <u>commutation semigroups</u> of G . Clearly a word of length n in $P(G)$ $(\Lambda(G))$ maps an element $g \in G$ to a left-normed (right-normed) commutator of weight $n + 1$ with first entry g .

The operations $\rho(x)$ and $\lambda(x)$ are important tools of group theory. The difference of behaviour of these two operations is probably widely known. But while certain aspects of it and specific examples can be found in the literature (cf. e.g. HEINEKEN [12]), no connected account seems to exist. A question that naturally arises is : Are the commutation semigroups of a group isomorphic? Our investigations start by a simple observation that for D_6 , the dihedral group of order 6, we have $|P(D_6)| = 6$, $|\Lambda(D_6)| = 9$ and $P(D_6) \subset \Lambda(D_6)$; thereby providing a negative answer to the above question. We illustrate this example as follows :

ij - Table

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	3	1	5	6	4
3	3	1	2	6	4	5
4	4	6	5	1	3	2
5	5	4	6	2	1	3
6	6	5	4	3	2	1

I

$i\rho(j)$ - Table

	$\rho(1)$	$\rho(2)$	$\rho(3)$	$\rho(4)$	$\rho(5)$	$\rho(6)$
1	1	1	1	1	1	1
2	1	1	1	2	2	2
3	1	1	1	3	3	3
4	1	3	2	1	2	3
5	1	3	2	3	1	2
6	1	3	2	2	3	1

II

$i\lambda(j)$ - Table

	$\lambda(1)$	$\lambda(2)$	$\lambda(3)$	$\lambda(4)$	$\lambda(5)$	$\lambda(6)$
1	1	1	1	1	1	1
2	1	1	1	3	3	3
3	1	1	1	2	2	2
4	1	2	3	1	3	2
5	1	2	3	2	1	3
6	1	2	3	3	2	1

III

The tables I, II and III on page ix are respectively the ij table, $i\rho(j)$ table and $i\lambda(j)$ table of D_6.

$\rho(D_6)$ has the following six elements:

$$\rho(1),\ \rho(2),\ \rho(3),\ \rho(4),\ \rho(5),\ \rho(6)\ .$$

$\Lambda(D_6)$ has the following nine elements:

$$\lambda(1),\ \lambda(2),\ \lambda(3),\ \lambda(4),\ \lambda(5),\ \lambda(6),\ \lambda^2(4),\ \lambda^2(5),\ \lambda^2(6)\ .$$

Further, since $\rho(1) = \lambda(1)$, $\rho(2) = \lambda(3)$, $\rho(3) = \lambda(2)$, $\rho(4) = \lambda^2(4)$, $\rho(5) = \lambda^2(5)$ and $\rho(6) = \lambda^2(6)$, we have $\rho(D_6) \subset \Lambda(D_6)$.

Among dihedral groups D_{2n}, one also finds examples where $\Lambda \subset \rho$ (e.g. D_{14}) ; $\rho \equiv \Lambda$ (eg. D_{10}) ; $|\rho| = |\Lambda|$ but $\rho \not\equiv \Lambda$ (eg. D_{30}) etc. etc. In fact we give a criterion of isomorphism of the commutation semigroups of D_{2n} (Theorem 2.1). We also give a criterion of proper inclusion of these two semigroups (Theorem 2.3).

For nilpotent groups among the dihedral groups, it turns out (Theorem 2.1) that the commutation semigroups are isomorphic; and one would expect them to be isomorphic for nilpotent groups in general. This, however, is again not true; not even for groups which are both nilpotent and metabelian. In fact we prove that for every integer $n \geqq 5$, there is a finite metabelian nilpotent group of class precisely n whose commutation semigroups are not isomorphic (Theorems 4.2 and 4.3). For groups of class 2, these semigroups are identical and for class 3 they are isomorphic. The problem is yet undecided for nilpotent groups of class 4; however we show that in this case the commutation semigroups have the same cardinality (Theorem 4.1).

If in addition to the multiplication of mappings of G into G, we also define an operation of "addition" (not necessarily commutative) of mappings by the rule $g(\theta_1 + \theta_2) = g\theta_1 . g\theta_2$, then the algebraic system of mappings closed with respect to these two operations forms a left distributive near-ring $\underline{\underline{N}}(G)$ (cf. BLACKETT [2]). Let $\underline{\underline{M}}(G)$ denote the sub near-ring of $\underline{\underline{N}}(G)$ generated by all ρ's and λ's. Let $\underline{\underline{R}}(G)$ be the algebraic system generated by ρ's only and $\underline{\underline{L}}(G)$ be generated by λ's only. Then $\underline{\underline{R}}(G)$ is itself a near-ring and it coincides with $\underline{\underline{M}}(G)$, while $\underline{\underline{L}}(G)$ is not always a near-ring since the closure with respect to subtraction is not guaranteed (Theorem 3.2); but if it is, then it also coincides with $\underline{\underline{M}}(G)$. If each element of a group G is a left-Engel element or if the derived group of G is periodic then $\underline{\underline{L}}(G)$ is a near-ring (Theorem 3.3).

A necessary and sufficient condition for $\underline{\underline{M}}(G)$ to be a ring is that G be 3-metabelian* (Theorem 3.4). Thus if G is metabelian (3-metabelian) it is convenient to carry out all commutator calculations inside $\underline{\underline{M}}(G)$. This is why in Chapter IV we do most of our calculations in $\underline{\underline{M}}(G)$; the simplicity of the

---

* A group G is called 3-metabelian if every 3 generated subgroup of G is metabelian (see page 6).

arguments thus becomes evident.

Apart from the present chapter, there are six chapters in this thesis. Chapter I is also introductory and this together with the present chapter contains all notations, definitions and results which have been repeatedly used in the rest of the thesis.

In Chapter III we study the structure of the commutation near-ring $\underline{\underline{M}}(G)$. Two main results of this chapter are : (i) the criterion for $\underline{\underline{M}}(G)$ to be a ring and (ii) the criterion for multiplication in $\underline{\underline{M}}(G)$ to be commutative.

Chapters II and IV are devoted to the study of the commutation semigroups. While Chapter II deals with dihedral groups, Chapter IV deals with nilpotent groups.

Chapters V and VI are of independent interest. In Chapter V we consider some two variable commutator laws and show their equivalence to the commutative law $[x,y] = 1$. In Chapter VI we consider groups satisfying the law $x\rho^{m}(y) = x\rho^{m+1}(y)$. For these groups it is shown that every element of odd order is an mth left Engel element and if no element of $\gamma_{m+1}(G)$ has order 3 then G satisfies the mth Engel condition. We conclude the Chapter by proving that a finite group satisfying the above law is soluble. The case $m = 2$ has been discussed in detail in [7] and there some results for the case $m = 3$ are also given. Other results concerning the groups satisfying the law $x\rho^m(y) = x\rho^{m+n}(y)$ or $x\lambda^m(y) = x\lambda^{m+n}(y)$ are given in [8] and [9].

CHAPTER I

1.1 NOTATION

As usual we write $x^y = y^{-1}xy$,

$[x,y] = x^{-1}y^{-1}xy$ and $[x,y,z] = [[x,y],z]$;

further $[x,oy] = x$ and $[x,ky] = [x,(k-1)y,y]$ for all $k \geq 1$. Thus $[x,y] = x\rho(y) = y\lambda(x)$ and $[x,ky] = x\rho^k(y)$.

The i-th term of the lower central series of a group G is denoted by $\gamma_i(G)$, and we have the following relation (cf. HALL [11] Page 156) :

1.1.1 $$[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G) \quad .$$

If A is a subgroup of a group G then we denote by $C(A)$ the centralizer of A in G . The centre of the group G is denoted by $Z(G)$ and $G' = \gamma_2(G)$ is the derived group of G .

1.2 COMMUTATOR IDENTITIES

The following commutator identities are standard or else can be directly verified:

1.2.1 $xy = yx[x,y] = [x^{-1},y^{-1}]yx$,

1.2.2 $x^y = x[x,y]$,

1.2.3 $[x,y] = [y,x]^{-1}$

1.2.4 $[x,y]^z = [x^z,y^z]$,

1.2.5 $[x,y] = [y^{-1},x]^y = [x,y^{-1}]^{-y}$,

1.2.6 $[x,y] = [y,x^{-1}]^x = [x^{-1},y]^{-x}$,

1.2.7 $[xy,z] = [x,z]^y[y,z]$,

1.2.8 $[x,yz] = [x,z][x,y]^z$,

1.2.9 $[x,y^{-1},z]^y[y,z^{-1},x]^z[z,x^{-1},y]^x = 1$,

1.2.10* $[x,y,z^x][z,x,y^z][y,z,x^y] = 1$.

In continuation we list some other implications:

1.2.11 If $x \in \gamma_i(G)$, $y \in \gamma_j(G)$ then

$x^y = x \bmod \gamma_{i+j}(G)$ (by 1.2.2 and 1.1.1)

1.2.12 If G is a metabelian group, then

$$[x,y,z,w] = [x,y,w,z]$$

for all x, y, z, w in G .

1.2.13 In metabelian groups

$$[x,y^n] = \prod_{k=1}^{n} [x,ky]^{\binom{n}{k}}$$

---

*

By using 1.2.5, 1.2.9 gives

$$[[y,x]^{y^{-1}},z]^y[[z,y]^{z^{-1}},x]^z[[x,z]^{x^{-1}},y]^x = 1$$

which on interchanging x and y , and using 1.2.4 gives 1.2.10.

1.2.14 If $y \in C(G')$, then

(i) $[x,y^n] = [x,y]^n$ for all integers n,

(ii) $[x,zy] = [x,z][x,y]$.

1.2.15 If G is a metabelian group and if $[x,y] = 1$ for some $x,y \in G$, then for all $g \in G$,

$[x,g,y] = [y,g,x] = [x,[g,y]]$.

1.3 IDENTITIES AND RESULTS FOR THE NEAR-RING $\underline{\underline{M}}(G)$.

For $z \in Z(G)$, each of the mappings $\rho(z)$ and $\lambda(z)$ is the zero mapping, i.e. the mapping which takes every element of the group onto 1. We denote this mapping by the symbol "0". Also we write $g(-\theta) = (g\theta)^{-1}$ whenever $\theta \in \underline{\underline{M}}(G)$. The following identities and implications in $\underline{\underline{M}}(G)$ are consequences of the identities in §1.2:

1.3.1 $\rho(x) + \lambda(x) = 0$ (by 1.2.3),

1.3.2 $\rho(x) = \lambda(x^{-1}) + \lambda(x^{-1})\rho(x)$ (by 1.2.5),

1.3.3 $\lambda(x) = \rho(x^{-1}) + \rho(x^{-1})\rho(x)$ (by 1.2.6),

1.3.4 $\rho(xy) = \rho(y) + \rho(x) + \rho(x)\rho(y)$ (by 1.2.8),

1.3.5 $\lambda(xy) = \lambda(x) + \lambda(x)\rho(y) + \lambda(y)$ (by 1.2.7),

1.3.6 $\rho(x)\rho(y) = \lambda(x) + \lambda(x)\lambda(y) + \rho(x)$.

<u>Proof</u>. $g\rho(x)\rho(y) = [g,x,y] = [y,[x,g]]^{[g,x]}$ (by 1.2.6)

$= [x,g]\ [y,[x,g]]\ [g,x] \quad = \quad g(\lambda(x) + \lambda(x)\lambda(y) + \rho(x))$.

1.3.7 $\quad (\theta_1 + \theta_2)\rho(x) = -\theta_2 + \theta_1\rho(x) + \theta_2 + \theta_2\rho(x)$

for $\theta_1, \theta_2 \in \underline{\underline{M}}(G)$.

__Proof.__ $\quad g(\theta_1 + \theta_2)\rho(x) \quad = \quad [g\theta_1 . g\theta_2, x]$

$= [g\theta_1, x]^{g\theta_2}[g\theta_2, x] \quad = \quad (g\theta_2)^{-1}[g\theta_1, x]g\theta_2[g\theta_2, x]$

$= g(-\theta_2 + \theta_1\rho(x) + \theta_2 + \theta_2\rho(x))$.

1.3.8 $\quad (\theta_1 + \theta_2)\lambda(x) \quad = \quad \theta_2\lambda(x) - \theta_2 + \theta_1\lambda(x) + \theta_2$

for $\theta_1, \theta_2 \in \underline{\underline{M}}(G)$.

The proof is similar.

1.3.9 $\quad$ If G is metabelian, then

$\rho(x^n) \quad = \quad \Sigma_{i=1}^{n} \binom{n}{i} \rho^i(x)$ (by 1.2.13).

1.3.10 $\quad$ If $x \in C(G')$, then

$\rho(x^n) \quad = \quad n\rho(x)$ (by 1.2.14(i)).

1.3.11 $\quad$ If $y_i \in C(G')$, then

$\rho(x, y_1 \ldots y_n) \quad = \quad \rho(x) + \Sigma_{i=1}^{n} \rho(y_i)$ (by 1.2.14(ii) used repeatedly).

1.4 __SOME RESULTS FOR NILPOTENT__ $\underline{\underline{M}}(G)$

Let $\pi_n \in \underline{\underline{M}}(G)$ denote a product of length n in ρ's and λ's $(g\pi_o = g)$. If G is nilpotent of class c then for $n \geqq c$, $\pi_n = 0$, and we prove the following:

1.4.1 $\quad$ If $i + j + 1 \geqq c$, then $\pi_i + \pi_j \quad = \quad \pi_j + \pi_i$.

Proof. Since $[g\pi_i, g\pi_j] \in \gamma_{i+j+2}(G)$ (by 1.1.1), we have $g\pi_i . g\pi_j = g\pi_j . g\pi_i$ which gives $g(\pi_i + \pi_j) = g(\pi_j + \pi_i)$.

1.4.2 If $x \in \gamma_i(G)$, $y \in \gamma_j(G)$, then

$$(xy)\pi_k = x\pi_k . y\pi_k \mod \gamma_{i+j+k}(G) .$$

Proof. The proof is by induction on k . When $k = 0$, the result is given. Suppose the result is true for all integers less than k . Write $\pi_k = \pi_{k-1}\,\alpha(z)$ where $\alpha(z) \in \{\rho(z), \lambda(z)\}$. Then by induction hypothesis $(xy)\pi_{k-1}.\alpha(z)$

$= [x\pi_{k-1} . y\pi_{k-1} . u, z]^{\varepsilon}$ (where $u \in \gamma_{i+j+k-1}(G)$ and $\varepsilon = +1$ or -1 according as $\alpha(z)$ is $\rho(z)$ or $\lambda(z)$)

$= [x\pi_{k-1} . y\pi_{k-1}, z]^{\varepsilon} \mod \gamma_{i+j+k}(G)$ (by 1.2.11)

$= ([x\pi_{k-1}, z][y\pi_{k-1}, z])^{\varepsilon} \mod \gamma_{i+j+k}(G)$ (by 1.2.7)

$= x\pi_{k-1}\alpha(z) . y\pi_{k-1}\alpha(z) \mod \gamma_{i+j+k}(G)$

$= x\pi_k . y\pi_k \mod \gamma_{i+j+k}(G)$.

We can now prove the following results when G is nilpotent of class c:

1.4.3 $(\pi_i + \pi_j)\pi_k = \pi_i\pi_k + \pi_j\pi_k$ if $i + j + k + 1 \geqq c$.

Proof. By 1.4.2 we have,

$$\begin{aligned}(g\pi_i . g\pi_j)\pi_k &= g\pi_i\pi_k . g\pi_j\pi_k \mod \gamma_{i+j+k+2}(G)\\ &= g(\pi_i\pi_k + \pi_j\pi_k) .\end{aligned}$$

1.4.4 $\pi_i\,\rho(x)\pi_j = \pi_i\,\lambda(x^{-1})\pi_j$ if $i + j + 2 \geqq c$.

Proof. We have

$$g\pi_i\rho(x)\pi_j = g\pi_i(\lambda(x^{-1}) + \lambda(x^{-1})\rho(x))\pi_j \qquad \text{(by 1.3.2)}$$

$$= (g\pi_i\lambda(x^{-1}).g\pi_i\lambda(x^{-1})\rho(x))\pi_j$$

$$= g\pi_i\lambda(x^{-1})\pi_j \, g\pi_i\lambda(x^{-1})\rho(x)\pi_j \mod \gamma_{2i+j+5}(G) \qquad \text{(by 1.4.2)}$$

$$= g\pi_i\lambda(x^{-1})\pi_j \mod \gamma_{i+j+3}(G)$$

$$= g\pi_i\lambda(x^{-1})\pi_j \; .$$

1.5 SOME DEFINITIONS AND LEMMAS.

An element $x \in G$ is called an mth left Engel element if $\rho^m(x) = 0$. [It may be noted that for any $x \in G$, $\rho^m(x) = 0$ and $\lambda^m(x^{-1}) = 0$ are equivalent. Defining $gw(x) = g^x$, by 1.2.5 it follows that $\rho(x) = \lambda(x^{-1})w(x)$ and since by 1.2.4 $[x^{-1},g]^x = [x^{-1},g^x]$, it follows that $\lambda(x^{-1})w(x) = w(x)\lambda(x^{-1})$. Thus $\rho^m(x) = (\lambda(x^{-1})w(x))^m = \lambda^m(x^{-1})w(x^m)$, so that if $\rho^m(x) = 0$ we have $\lambda^m(x^{-1}) = 0$ and conversely. BAER [1], HEINEKEN [13] and some others use "$\lambda^m(x) = 0$" as the definition of mth left Engel element.] A group G is said to satisfy the mth Engel condition if $\rho^m(x) = 0$ for all $x \in G$ (and hence equivalently $\lambda^m(x) = 0$ for all $x \in G$) ; and we say that G is an E_m-group.

A group is called n-metabelian if every subgroup with n (or fewer) generators is metabelian. Obviously every 4-metabelian group is metabelian. NEUMANN [19] has shown the existence of 2-metabelian groups which are not 3-metabelian groups; and 3-metabelian groups which are not metabelian. Also we have the following lemmas:

Lemma 1.5.1 (HIGMAN [14]) A group is 2-metabelian if and only if it satisfies the law $[[x,y],[x,y^{-1}]] = 1$.

Lemma 1.5.2 (MACDONALD [18]) A group is 3-metabelian if and only if it satisfies the law $[[x,y],[x,z]] = 1$.

Lemma 1.5.3 (HEINEKEN [13]) An E_3-group is 2-metabelian.

Lemma 1.5.4 An element $x \in G$ is a 2nd left Engel element of G if and only if the normal closure of x in G, is abelian.

(This lemma has been recorded in [3] without proof. However the proof is straight forward.)

A particular case of a theorem of BAER [1], is the following lemma:

Lemma 1.5.5. If x is a left Engel element of a finite group G then x is contained in the Fitting subgroup* of G .

---

* The Fitting subgroup is the maximal normal nilpotent subgroup of G .

Some very elementary facts from the number theory will be required in Chapter II. Let m,n be positive integers and denote by $\operatorname{ind}_m n$, $\operatorname{ind}_m^* n$ respectively, the least positive solution x, if such a solution exists, of the congruence

$$n^x \equiv 1 \pmod m, \quad n^x \equiv -1 \pmod m .$$

Then we have the following lemma:

<u>Lemma</u> 1.5.6 If m,n are relatively prime integers (clearly a necessary condition for the existence of $\operatorname{ind}_m n$ and $\operatorname{ind}_m^* n$ and also sufficient for the existence of $\operatorname{ind}_m n$), then

(i) if $\operatorname{ind}_m^* n$ exists then $\operatorname{ind}_m n$ is even, and in fact $\operatorname{ind}_m n = 2 \operatorname{ind}_m^* n$;

(ii) if $\operatorname{ind}_m^* -n$ exists and is even, then $\operatorname{ind}_m^* n$ exists and is equal to $\operatorname{ind}_m^* -n$;

(iii) if $\operatorname{ind}_m^* -n$ exists and is odd, then $\operatorname{ind}_m^* -n = \operatorname{ind}_m n$, and $\operatorname{ind}_m^* n$ does not exist.

<u>Proof</u>. We simplify the notation by putting $\operatorname{ind}_m n = r$, $\operatorname{ind}_m^* n = s$ and $\operatorname{ind}_m^* -n = t$. We first remark that if $n^x \equiv 1 \pmod m$ then x is a multiple of r; and if $n^x \equiv -1 \pmod m$ then x is an odd multiple of s. To prove (i), we assume that s exists. Then

$$n^{2s} \equiv 1 \pmod m, \quad \text{hence } r/2s .$$

Also

$$n^{r-s} \equiv -1 \pmod m , \quad \text{hence} \quad r - s$$

is an odd multiple of s , that is to say $2s/r$. It follows that $r = 2s$, as claimed.

To prove (ii) we assume that t exists and is even. Then $-1 \equiv (-n)^t \equiv n^t \pmod m$, hence s exists and t is an odd multiple of s ; as t is even, s is also even, and so

$$-1 \equiv n^s \equiv (-n)^s \pmod m \quad .$$

By the minimality of s and t we have $s = t$, as claimed.

To prove (iii) we assume that t exists and is odd. Then

$$n^t \equiv -(-n)^t \equiv 1 \pmod m \quad ,$$

hence t is a multiple of r , hence by (i) s does not exist; moreover

$$(-n)^r \equiv -n^r \equiv -1 \pmod m \quad ,$$

hence by the minimality of r and t , we have $r = t$, and the lemma is proved.

CHAPTER II

THE COMMUTATION SEMIGROUPS OF DIHEDRAL GROUPS

INTRODUCTION

It was shown on page x that $\rho(D_6) \not\cong \Lambda(D_6)$. In this Chapter we continue the study of commutation semigroups of dihedral groups in general. We give criteria of isomorphism and of proper inclusion of these semigroups.

PRELIMINARIES

Let $n = 2^r m$ be a fixed positive integer where m is odd and $r \geqq 0$. Let G be the dihedral group of order $2n$ given as :

$$(1) \quad G = gp\{a, b / b^n = 1 \; , \; a^2 = 1 \; , \; aba = b^{-1}\} \quad .$$

Each element of G can be uniquely written as b^k or ab^k for some integer k. Let N denote the set of all residue classes modulo n. For each pair of elements $i, j \in N$, define a mapping $\mu(i,j)$ of G into itself as follows:

$$(2) \quad b^k\mu(i,j) = b^{ki} \; , \; ab^k\mu(i,j) = b^{ki+j} \quad .$$

If $\mu(i,j) = \mu(i',j')$, then by (2) we have

$$b^{ki} = b^{ki'} \text{ and } b^{ki+j} = b^{ki'+j'} \quad ,$$

so that

$$i \equiv i' \pmod n \text{ and } j \equiv j' \pmod n \quad .$$

Thus we have

$$(3) \quad \mu(i,j) = \mu(i',j') \text{ if and only if } i = i' \text{ and } j = j' .$$

Also since

$$b^k\mu(i,j)\mu(i',j') = b^{ki}\mu(i',j') = b^{kii'}$$

and

$$ab^k\mu(i,j)\mu(i',j') = b^{ki+j}\mu(i',j') = b^{kii'+ji'} ,$$

it follows that

$$(4) \quad \mu(i,j)\mu(i',j') = \mu(ii',ji') .$$

With the multiplication given by (4) we observe that

$$\begin{aligned}(\mu(i,j)\mu(i',j'))\mu(i'',j'') &= \mu(ii',ji')\mu(i'',j'') \\ &= \mu(ii'i'',ji'i'') \\ &= \mu(i,j)\mu(i'i'',j'i'') \\ &= \mu(i,j)(\mu(i',j')\mu(i'',j'')) .\end{aligned}$$

Thus the set, say S , of all mappings $\mu(i,j)$ form a semigroup.

Now, since

$$b^k\rho(b^{-j}) = 1 = b^0$$

and

$$ab^k\rho(b^{-j}) = b^{-k}(ab^ja)b^kb^{-j} = b^{0-2j} ,$$

we have from (2) that

$$(5)\qquad \rho(b^{-j}) \;=\; \mu(0,-2j)\quad .$$

Further, since

$$b^{k}\rho(ab^{-j}) \;=\; b^{-k}b^{j}(ab^{k}a)b^{-j} \;=\; b^{-2k}$$

and

$$ab^{k}\rho(ab^{-j}) \;=\; b^{-k}(ab^{j}aab^{k}a)b^{-j} \;=\; b^{-2k-2j}\quad ,$$

we have from (2) that

$$(6)\qquad \rho(ab^{-j}) \;=\; \mu(-2,-2j)\quad .$$

From (5) and (6) it follows that

(7) $\rho(G)$ is a sub semigroup of the semigroup S and it consists of all elements of the form $\mu(0,(-2)^{\ell}j)$ and $\mu((-2)^{\ell},(-2)^{\ell}j)$, where $\ell \geqq 1$ (by (3) and (4)) . On the other hand since

$$b^{k}\lambda(b^{-j}) \;=\; 1 \;=\; b^{0}$$

and

$$ab^{k}\lambda(b^{-j}) \;=\; b^{j}b^{-k}(ab^{-j}a)b^{k} \;=\; b^{0+2j}\quad ,$$

we have from (2) that

$$(8)\qquad \lambda(b^{-j}) \;=\; \mu(0,2j)\quad .$$

Further, since

$$b^{k}\lambda(ab^{-j}) \;=\; b^{j}(ab^{-k}a)b^{-j}b^{k} \;=\; b^{2k}$$

and

$$ab^k\lambda(ab^{-j}) = b^j(ab^{-k}aab^{-j}a)b^k = b^{2k+2j} ,$$

we have from (2) that

$$(9) \qquad \lambda(ab^{-j}) = \mu(2,2j) .$$

From (8) and (9) it follows that

(10) $\Lambda(G)$ is a subsemigroup of the semigroup S and it consists of all elements of the form $\mu(0,2^\ell j)$ and $\mu(2^\ell,2^\ell j)$, where $\ell \geqq 1$ (by (3) and (4)).

Now let $P_1(\Lambda_1)$ denote the set of all elements of $P(G)(\Lambda(G))$ which are of the form $\mu(0,(-2)^\ell j)$ $(\mu(0,2^\ell j))$; and let $P_2 = P(G)\setminus P_1$ $(\Lambda_2 = \Lambda(G)\setminus\Lambda_1)$. Since

$$\mu(0,2^\ell j) = \mu(0,(-2)^\ell(-1)^\ell j) ,$$

it follows that

$$(11) \quad P_1 = \Lambda_1 .$$

For each $i = 1,2,\ldots,$ let $P_2^{(i)}$ denote the set of all elements $\mu((-2)^i,(-2)^i j)$ of P_2 where $j = 1,2\ldots$; and let $\Lambda_2^{(i)}$ denote the corresponding set of all elements $\mu(2^i,2^i j)$ of Λ_2 where $j = 1,2,\ldots$. By (3), $\mu((-2)^i, (-2)^i j) = \mu((-2)^i,(-2)^i j')$ implies that $(-2)^i j \equiv (-2)^i j' \pmod n$, which gives $j' \equiv j + 2^{r-i}m$ (where $2^{r-i} = 1$ if $i \geqq r$) and conversely. Similarly $\mu(2^i,2^i j) = \mu(2^i,2^i j')$ implies that $j' \equiv j+2^{r-i}m$ and conversely.

Thus we have

$$(12) \qquad |\rho_2^{(i)}| = |\Lambda_2^{(i)}| = 2^{r-i}m \ ,$$

where $2^{r-i} = 1$ if $i \geqq r$.

If $\mathrm{ind}_m -2 = s$ i.e. if s is the least positive integer such that $(-2)^s \equiv 1 \pmod m$, then $(-2)^{r+s} \equiv (-2)^r \pmod{2^r m}$. Thus by (3) we have

$$\mu((-2)^r,(-2)^r j) = \mu((-2)^{r+s},(-2)^{r+s} j)$$

so that

$$\rho_2^{(r)} = \rho_2^{(r+s)} \quad .$$

Hence we have the following disjoint partition of ρ_2 :

$$(13) \qquad \rho_2 = \rho_2^{(1)} \cup \ldots\ldots\ldots \cup \rho_2^{(r-1)} \cup \rho_2^{(r)} \cup \ \ldots \cup \rho_2^{(r+s-1)}$$

where $s = \mathrm{ind}_m -2$ and $r \geqq 2$;

and when $r = 0$ or 1 , as a special case we have the following partition of ρ_2 :

$$(13)^* \quad \rho_2 = \rho_2^{(1)} \cup \ldots\ldots \cup \rho_2^{(s)}$$

Similarly if $\mathrm{ind}_m 2 = t$ i.e. if t is the least positive integer such that $2^t \equiv 1 \pmod m$, then $2^{r+t} \equiv 2^r \pmod{2^r m}$. Thus by (3) we have

$$\mu(2^r,2^r j) = \mu(2^{r+t},2^{r+t} j)$$

so that

$$\Lambda_2^{(r)} = \Lambda_2^{(r+t)} \quad ;$$

and as before we have the following partition of Λ_2 :

$$(14) \quad \Lambda_2 = \Lambda_2^{(1)} \cup \ldots \cup \Lambda_2^{(r-1)} \cup \Lambda_2^{(r)} \cup \ldots \cup \Lambda_2^{(r+t-1)}$$

where $t = \mathrm{ind}_m 2$ and $r \geqq 2$; and when $r = 0$ or 1 , as a special case we have the following partition of Λ_2 :

$$(14)^* \quad \Lambda_2 = \Lambda_2^{(1)} \cup \ldots \cup \Lambda_2^{(t)} \quad .$$

From (12), (13), $(13)^*$, (14), $(14)^*$ it follows that

$$(15) \quad |P_2| = \Sigma_{i=1}^{r-1} 2^{r-i} m + ms \qquad \text{when } r \geqq 2$$

$$= ms \qquad \text{when } r = 0 , 1$$

and

$$|\Lambda_2| = \Sigma_{i=1}^{r-1} 2^{r-i} m + mt \qquad \text{when } r \geqq 2 ,$$

$$= mt \qquad \text{when } r = 0 . 1$$

From (11) and (15) it follows that

(16) If $|P(G)| = |\Lambda(G)|$ then

$$\mathrm{ind}_m 2 = \mathrm{ind}_m -2 \quad .$$

Now we can prove the following theorem :

<u>THEOREM</u> 2.1 Let $n = 2^r m$ be a fixed positive integer and let G be the dihedral group of order $2n$; then $P(G) \cong \Lambda(G)$

if and only if $\operatorname{ind}_p 2 \equiv 0 \pmod 4$ for each prime divisor p of m.

<u>Proof</u>. Let η be an isomorphism of $P(G)$ onto $\Lambda(G)$. If $m = 1$, there is nothing to prove. Let $m > 1$ and let T denote the subset of N (the set of all residue classes modulo n) with elements of the form $2j$.

Since by (2)

$$b^k\mu(0,0) = b^0 = 1 \quad \text{and} \quad ab^k\mu(0,0) = b^0 = 1 ,$$

it follows that

$$\mu(0,0)\eta = \mu(0,0)$$

(since $\mu(0,0)$ is the zero element of $P(G)$ and $\Lambda(G)$). Also since for all i, $\mu((-2)^i,(-2)^i j)\mu(u,v) = \mu(0,0)$ implies by (2) that $\mu((-2)^i u,(-2)^i ju) = \mu(0,0)$, we have by (3) that $u = 0$. Thus the equation $P(G)\mu(u,v) = \mu(0,0)$ is satisfied precisely when $u = 0$ for $\mu(u,v) \in P(G) \cup \Lambda(G)$. Further since by (7) ((10)) $\mu(i,j) \in P(G)$ $(\Lambda(G))$ implies that $i,j \in T$, we have

$$(17) \qquad \mu(0,v)\eta = \mu(0,\theta(v))$$

for some permutation θ of T.

Suppose $\mu(-2,0)\eta = \mu(c,e)$, then by (10) $c = 2^\ell$ for some ℓ; and for all $t = 1,2,\ldots,$ $\mu^t(-2,0)\eta = \mu^t(c,e)$. Thus

$$(\mu(0,v)\mu^t(-2,0))\eta \;=\; \mu(0,\theta(v))\mu^t(c,e)$$

gives in turn

$$(\mu(0,v)\mu((-2)^t,0))\eta \;=\; \mu(0,\theta(v))\mu(c^t,ec^{t-1}) \quad \text{by (4)} ;$$

$$\mu(0,v(-2)^t)\eta \;=\; \mu(0,c^t\theta(v)) \quad .$$

And in particular, since θ is $1-1$, we have for all $t = 1,2,\ldots,$ that the equations

$$(18) \qquad ((-2)^t-1)x \;=\; 0 \quad \text{and} \quad (c^t-1)x \;=\; 0$$

have the same number of solutions $x \in T$. Further since $\mu(-2,0)\eta = \mu(c,e)$, both $\mu(-2,0)$ and $\mu(c,e)$ generate cyclic subsemigroups of the same order ; in other words $(-2)^r \equiv (-2)^{r+s}$ (mod n) if and only if $c^r \equiv c^{r+s}$ (mod n) and equivalently $\mathrm{ind}_m -2 = \mathrm{ind}_m c$. By (16) we also have $\mathrm{ind}_m -2 = \mathrm{ind}_m 2$, so that $\mathrm{ind}_m 2 = \mathrm{ind}_m c$ and hence 2 is a power of c. But c is already a power of 2, so that $c \equiv 2 \pmod m$. Thus from (18) we have that the equations

$$(19) \qquad ((-2)^t-1)x \;=\; 0 \quad \text{and} \quad (2^t-1)x \;=\; 0$$

have the same number of solutions $x \in T$.

Let $d_1 = ((-2)^t-1,n)$ and $d_2 = (2^t-1,n)$, then the number of solutions of the equations (19) are $\cancel{\varepsilon}\, d_1$ and $\cancel{\varepsilon}\, d_2$ respectively. ~~where $\varepsilon = \frac{1}{2}$ or 1 according as n is even or odd.~~

In particular, when t is odd we have $d_1 = (2^t + 1, n)$ and $d_2 = (2^t - 1, n)$, so that

$$(20) \quad (2^t + 1, n) = (2^t - 1, n) = (2^{2t} - 1, n) = 1$$

for all positive odd integers t.

Now let $1 \neq p$ be a prime divisor of m. If $\mathrm{ind}_p 2 \not\equiv 0 \pmod 4$, there is an odd or twice-an-odd positive integer s such that $2^s - 1 \equiv 0 \pmod p$ and also since $n \equiv 0 \pmod p$, we have $(2^s - 1, n) \equiv 0 \pmod p$ which is contrary to (20) since $p \neq 1$. This completes the proof of the first part of the Theorem 2.1.

Conversely suppose that $\mathrm{ind}_p 2 \equiv 0 \pmod 4$ for each prime divisor p of m, then we shall prove that $P(G) \cong A(G)$. Let $0 \neq k \in N$ (the set of all residue classes modulo n) and let $d = (k, m)$.

If $d < m$, the residue classes modulo m/d which are prime to m/d form a multiplicative group H of order $\Phi(m/d)$, the Euler's function of m/d. Let C_1 and C_2 denote the cyclic subgroups of H generated by 2 and -2 respectively. Since $\mathrm{ind}_p 2 \equiv 0 \pmod 4$, we have in particular $\mathrm{ind}_p 2 = \mathrm{ind}_p -2$ for each prime divisor p of m. Thus C_1 and C_2 are of the same even order. Clearly either $C_1 = C_2$ or else $C_1 C_2 = C_1 \cup -4C_1 = C_2 \cup -4C_2$; and in the later case if $\{s_1 (=1), s_2, \ldots, s_q\}$ is a set of coset representatives of $C_1 C_2$ in H, then

$\{s_1(=1), s_2, \ldots, s_q, -4s_1, -4s_2, \ldots, -4s_q\}$ is a set of common coset representatives of C_1 and C_2 in H. In either of the cases there is a set, say M, of common coset representatives of C_1 and C_2 in H. Thus k can be written as,

(21) $$k = (-2)^{t_1}\ell_1 = 2^{t_2}\ell_2$$

for some $\ell_1, \ell_2 \in M$, where ℓ_1, ℓ_2, t_1, t_2 are uniquely determined; and t_1, t_2 are either both even or both odd (because if one of them, say t_2, is even then $2^{t_2}\ell_2 = (-2)^{t_2}\ell_1$ and hence $t_1 = t_2$, $\ell_1 = \ell_2$).

Now we define, for each $k \in N$, integers $\alpha(k), \beta(k) \in N$ as follows:

(22) (i) $\alpha(0) = \beta(0) = 0$;

(ii) $\alpha(k) = \beta(k) = (-1)^t k$ if $d = m$ and $k \neq 0$,

where t is the largest power of 2 dividing k

(Thus $\alpha(-k) = \beta(-k) = -(-1)^t k = -\alpha(k) = -\beta(k)$) ;

(iii) $\alpha(k) = (-1)^{t_1} k$ and $\beta(k) = (-1)^{t_2} k$

if $d < m$ and $k \neq 0$

where t_1, t_2 are given by (21)

(Thus $\alpha(-k) = -(-1)^{t_1} k = -\alpha(k)$ and $\beta(-k) = -(-1)^{t_2} k = -\beta(k)$).

From (22) (ii) and (iii) we have,

(23) $$\alpha(1) = \beta(1) = 1$$

and

$$(24) \qquad \begin{cases} \alpha(k) = \alpha(k') & \text{if and only if} \quad k = k' \\ \beta(k) = \beta(k') \end{cases}$$

When $d = m$, by 22 (ii), $\alpha((-2)^{\ell}k) = (-1)^{\ell}\alpha(2^{\ell}k) = (-1)^{\ell}.(-1)^{\ell+t}.2^{\ell}k$ where t is the largest power of 2 dividing k. Thus $\alpha((-2)^{\ell}k) = (-1)^{t}2^{\ell}k = 2^{\ell}\alpha(k)$. Similarly when $d = m$ we have $\beta(-2)^{\ell}k) = 2^{\ell}\beta(k)$.

When $d < m$, by 22 (iii),
$\alpha((-2)^{\ell}k) = (-1)^{\ell}\alpha(2^{\ell}k) = (-1)^{\ell}.(-1)^{\ell+t_1}.2^{\ell}k = (-1)^{t_1}2^{\ell}k = 2^{\ell}\alpha(k)$
where t_1 is given by (21). Also by 22 (iii),
$\beta((-2)^{\ell}k) = (-1)^{\ell}\beta(2^{\ell}k) = (-1)^{\ell}.(-1)^{\ell+t_2}.2^{\ell}k = (-1)^{t_2}2^{\ell}k = 2^{\ell}\beta(k)$
where t_2 is given by (21). Thus we have shown that

$$(25) \qquad \alpha((-2)^{\ell}k) = 2^{\ell}\alpha(k) \quad \text{and} \quad \beta((-2)^{\ell}k) = 2^{\ell}\beta(k) \quad .$$

Finally when $d = m$, by 22 (ii) we have
$\alpha(\beta(k)) = \beta(\alpha(k)) = \alpha(\alpha(k)) = \alpha((-1)^{t}k) = (-1)^{t}\alpha(k) = (-1)^{t}.(-1)^{t}k$
$= (-1)^{2t}k = k$ where t is the largest power of 2 dividing k.
And when $d < m$, by 22 (iii) we have,
$\alpha(\beta(k)) = \alpha((-1)^{t_2}k) = (-1)^{t_2}\alpha(k) = (-1)^{t_2}.(-1)^{t_1}k = (-1)^{t_1+t_2}k = k$
(since by (21), $t_1 + t_2$ is even). Also
$\beta(\alpha(k)) = \beta((-1)^{t_1}k) = (-1)^{t_1}\beta(k) = (-1)^{t_1}.(-1)^{t_2}k$
$= (-1)^{t_1+t_2}k = k$. Thus we have shown that,

$$(26) \qquad \alpha(\beta(k)) = \beta(\alpha(k)) = k \; .$$

Now we can prove the isomorphism of $\rho(G)$ and $\Lambda(G)$ as follows: We define mappings η_1 and η_2 of $\rho(G)$ into $\Lambda(G)$ and $\Lambda(G)$ into $\rho(G)$ respectively as

$$(27)\qquad \mu(u,v)\eta_1 = \mu(\alpha(u),\alpha(v))$$

$$\mu(u,v)\eta_2 = \mu(\beta(u),\beta(v)) .$$

By (23), (24) and (25), both η_1 and η_2 are well defined mappings and by (26) both η_1 and η_2 are inverses of one another, since $\mu(u,v)\eta_1\eta_2 = \mu(\alpha(u),\alpha(v))\eta_2 = \mu(\beta(\alpha(u)),\beta(\alpha(v))) = \mu(u,v)$ $= \mu(\alpha(\beta(u)),\alpha(\beta(v))) = \mu(\beta(u),\beta(v))\eta_1 = \mu(u,v)\eta_2\eta_1$. Thus to show that $\rho(G)$ and $\Lambda(G)$ are isomorphic, it is sufficient to show that η_1 is a homomorphic mapping. An arbitrary element of $\rho(G)$ has the form $\mu((-2)^k,(-2)^k j)$ or $\mu(0,(-2)^k j)$ by (7). Also

$$\mu((-2)^k,(-2)^k j)\eta_1 = \mu(\alpha(-2)^k,\alpha((-2)^k j))$$

$$= \mu(2^k\alpha(1),2^k\alpha(j)) \qquad \text{(by (25))}$$

$$= \mu(2^k,2^k\alpha(j)) \qquad \text{(by (23))} ;$$

and

$$\mu(0,(-2)^k j)\eta_1 = \mu(\alpha(0),\alpha((-2)^k j)) = \mu(0,2^k\alpha(j))$$
(by 22(i)).

Thus we have

$$(28)\qquad \mu((-2)^k,(-2)^k j)\eta_1 = \mu(2^k,2^k\alpha(j))$$

$$\mu((-2)^{k'},(-2)^{k'} j')\eta_1 = \mu(2^{k'},2^{k'}\alpha(j'))$$

$$\mu(0,(-2)^{k''} j'')\eta_1 = \mu(0,2^{k''}\alpha(j''))$$

Now

$$(\mu((-2)^k,(-2)^k j)\mu((-2)^{k'},(-2)^{k'}j'))\eta_1$$

$$= \mu((-2)^{k+k'},(-2)^{k+k'}j)\eta_1 \qquad \text{(by (4))}$$

$$= \mu(2^{k+k'},2^{k+k'}\alpha(j)) \qquad \text{(by (28))}$$

$$= \mu(2^k,2^k\alpha(j))\mu(2^{k'},2^{k'}\alpha(j')) \qquad \text{(by (4))}$$

and

$$(\mu(0,(-2)^{k''}j'')\mu((-2)^k,(-2)^k j))\eta_1$$

$$= \mu(0,(-2)^{k+k''}j'')\eta_1 \qquad \text{(by (4))}$$

$$= \mu(0,2^{k+k''}\alpha(j'')) \qquad \text{(by (28))}$$

$$= \mu(0,2^{k''}\alpha(j''))\mu(2^k,2^k\alpha(j) \qquad \text{(by (4))} \quad .$$

Thus it follows that η_1 is a homomorphism and hence an isomorphism of $P(G)$ onto $\Lambda(G)$. This completes the proof of the Theorem 2.1 .

Next we prove the following theorem .

THEOREM 2.2 Let $n = 2^r m$ be a fixed positive integer where m is odd and $r = 0,1$. Let G be the dihedral group of order $2n$. Then

(i) if $\text{ind}_m^* 2$ is even then $P(G) \equiv \Lambda(G)$;

(ii) if $\text{ind}_m^* {-2}$ is even then $P(G) \equiv \Lambda(G)$.

Proof of (i). Let $\mathrm{ind}^*_m 2 = s$, then, by hypothesis s is the least positive even integer such that $2^s \equiv -1 \pmod{m}$. Thus $2^{s+1} \equiv -2 \pmod{m}$ and hence equivalently $(-2)^{s+1} \equiv 2 \pmod{m}$ (since $s+1$ is odd). Thus if $r = 0$ or 1 then $2^{s+1} \equiv -2 \pmod{n}$ and $(-2)^{s+1} \equiv 2 \pmod{n}$. Now by (3),

$$\mu(0,(-2)^{\ell}j) = \mu(0,2^{\ell(s+1)}j) \quad ;$$

$$\mu(0,2^{\ell}j) = \mu(0,(-2)^{\ell(s+1)}j) \quad ;$$

$$\mu((-2)^{\ell},(-2)^{\ell}j) = \mu(2^{\ell(s+1)},2^{\ell(s+1)}j) \quad ;$$

$$\mu(2^{\ell},2^{\ell}j) = \mu((-2)^{\ell(s+1)},(-2)^{\ell(s+1)}j) \quad .$$

Hence by (7) and (10) it follows that each element of $P(G)$ is contained in $\Lambda(G)$ and conversely. Thus $P(G) \equiv \Lambda(G)$.

Proof of (ii). Let $\mathrm{ind}^*_m -2 = s$, then, by hypothesis, s is the least positive even integer such that $(-2)^s \equiv -1 \pmod{m}$. Thus $2^s \equiv -1 \pmod{m}$ which gives $2^{s+1} \equiv -2 \pmod{m}$ and $(-2)^{s+1} \equiv 2 \pmod{m}$ (since $s+1$ is odd). Thus the proof follows as before.

We use Theorem 2.2 to prove the following Theorem:

THEOREM 2.3. Let $n = 2^r m$ be a positive integer where m is odd and $r \geq 0$; and let G be the dihedral group of order $2n$. Then

(i) if $r = 0$ or 1, $\rho(G) \subset \Lambda(G)$ if and only if $\mathrm{ind}_m^* 2$ is odd ;

(ii) if $r = 0$ or 1, $\Lambda(G) \subset \rho(G)$ if and only if $\mathrm{ind}_m 2$ is odd ; and

(iii) if $r > 1$, the proper inclusion of commutation semigroups does not hold.

Proof of (i). Let $\rho(G) \subset \Lambda(G)$. Then since $\mu(-2,0) \in \rho(G) \subset \Lambda(G)$, it follows by (3) and (10), that $\mu(-2,0) = \mu(2^{\ell},0)$ for some integer ℓ. Thus by (3) again $2^{\ell} \equiv -2 \pmod m$ and hence $2^{\ell-1} \equiv -1 \pmod m$. Whence, firstly $\mathrm{ind}_m^* 2$ exists and secondly it is odd by Theorem 2.2 (i) (since $r = 0$ or 1 and since the inclusion is proper).

Conversely, if $\mathrm{ind}_m^* 2$ is odd, then there is a least positive odd integer s such that $2^s \equiv -1 \pmod m$ and hence $2^{s+1} \equiv -2 \pmod n$, since $r = 0$ or 1. Now

$$\mu(0,(-2)^{\ell} j) = \mu(0,2^{\ell(s+1)} j)$$

and

$$\mu((-2)^{\ell},(-2)^{\ell} j) = \mu(2^{\ell(s+1)},2^{\ell(s+1)} j)$$

imply by (7) and (10); that $\rho(G) \subseteq \Lambda(G)$. Thus to show that the inclusion is proper it is sufficient to show that $\mu(2,0)(\in\Lambda(G))$ is not in $\rho(G)$. Suppose $\mu(2,0) \in \rho(G)$, then by (3) and (7) it follows that $\mu(2,0) = \mu((-2)^{\ell},0)$ for some ℓ and again by (3) it follows that $(-2)^{\ell} \equiv 2 \pmod m$

and hence $(-2)^{\ell-1} \equiv -1 \pmod{m}$; which gives that $\operatorname{ind}_m^* -2$ is meaningful which is a contradiction by Lemma 1.5.6 (ii) and (iii).

Proof of (ii). Let $\Lambda(G) \subset \rho(G)$, then $\mu(2,0) \in \Lambda(G)$ implies that $\mu(2,0) \in \rho(G)$ and as before $\mu(2,0) = \mu((-2)^{\ell},0)$ for some ℓ . Thus $(-2)^{\ell} \equiv 2 \pmod{m}$ gives $(-2)^{\ell-1} \equiv -1 \pmod{m}$. Whence, firstly $\operatorname{ind}_m^* -2$ exists and secondly by Theorem 2.2 (ii) it is odd (since $r = 0$ or 1 and since the inclusion is proper). Thus there is an odd positive integer s such that $(-2)^s \equiv -1 \pmod{m}$, so that $2^s \equiv 1 \pmod{m}$ (since s is odd). Hence $\operatorname{ind}_m 2$ is odd, since it divides s .

Conversely, if $\operatorname{ind}_m 2$ is odd then for a least positive odd integer s , $2^s \equiv 1 \pmod{m}$. Thus $2^{s+1} \equiv 2 \pmod{m}$ and hence $(-2)^{s+1} \equiv 2 \pmod{m}$, since s is odd. Thus if $r = 0$ or 1 we have $(-2)^{s+1} \equiv 2 \pmod{n}$ which gives by (3) that

$$\mu(0,2^{\ell}j) = \mu(0,(-2)^{\ell(s+1)}j)$$

and

$$\mu(2^{\ell},2^{\ell}j) = \mu((-2)^{\ell(s+1)},(-2)^{\ell(s+1)}j) \quad ;$$

and by (7) and (10) it follows that $\Lambda(G) \subseteq \rho(G)$. Thus to show that the inclusion is proper it is sufficient to show that $\mu(-2,0)(\in\rho(G))$ is not in $\Lambda(G)$. Suppose $\mu(-2,0) \in \Lambda(G)$. Then as before it follows that $\mu(-2,0) = \mu(2^{\ell},0)$ for some ℓ , which gives that $2^{\ell} \equiv -2 \pmod{m}$ and further that

$2^{\ell-1} \equiv -1 \pmod{m}$. Thus $\operatorname{ind}_m^* 2$ is meaningful which is a contradiction by Lemma 1.5.6 (i).

<u>Proof of (iii)</u>. Since $n = 2^r m$, if $r > 1$ then $(-2)^t \not\equiv 2 \pmod{2^r m}$ and $2^t \not\equiv -2 \pmod{2^r m}$ for any t . Hence in particular we have simultaneously $\mu(2,0) \notin P(G)$ and $\mu(-2,0) \notin \Lambda(G)$. This completes the proof of the Theorem 2.3 .

<u>Remark</u>. With the methods used in this chapter we could possibly cover more wider class of groups namely, the metacyclic groups; but as it becomes too involved we do not attempt it here.

CHAPTER III

THE COMMUTATION NEAR-RINGS OF A GROUP

INTRODUCTION.

By definition of $\underline{\underline{M}}(G)$ each element of it is a certain word in ρ's and λ's. Since $\lambda(x) = \rho(x^{-1}) + \rho(x^{-1})\rho(x)$ (by 1.3.3), each such word may be written in terms of ρ's only. Consequently the algebraic system $\underline{\underline{R}}(G)$, generated by all mappings $\rho(x)$ and closed with respect to the operations of addition and multiplication, is also closed with respect to subtraction and it coincides with the near-ring $\underline{\underline{M}}(G)$. On the other hand there exists a group G such that the algebraic system $\underline{\underline{L}}(G)$, generated by all mappings $\lambda(x)$, is not closed with respect to subtraction and hence fails to be a near-ring; but if for a particular group G, $\underline{\underline{L}}(G)$ is also a near-ring then it coincides with $\underline{\underline{M}}(G)$ (Theorem 3.2). We next turn to the problems: When does $\underline{\underline{M}}(G)$ form a ring? and when is multiplication in $\underline{\underline{M}}(G)$ commutative? The necessary and sufficient conditions for $\underline{\underline{M}}(G)$ to be a ring is that G be a 3-metabelian group (Theorem 3.4); and the necessary and sufficient condition for multiplication in $\underline{\underline{M}}(G)$ to be commutative is that G be nilpotent of class 2 (Theorem 3.5).

LENGTH OF A WORD.

To simplify the arguments we introduce the notion of "length" of a word μ of $\underline{\underline{M}}(G)$. We define the length recursively as follows: The words of the form $\rho(x), \lambda(x), \ldots$ are of length 1 ; and if μ_i and μ_j are words of length i and j respectively, then $\mu_i + \mu_j$ and $\mu_i . \mu_j$ are both of length $i + j$. Thus an element of $\underline{\underline{M}}(G)$ may have several representations as words and hence several lengths (each for each word).

Next we prove the following lemma:

Lemma 3.1 Each element of $\underline{\underline{M}}(G)$ has a representation as a word of the form $\cancel{\Sigma\, \alpha(a_i)}$ ~~or~~ $\Sigma\, \theta_i \alpha(a_i)$, where $\alpha(a_i) \in \{\rho(a_i), \lambda(a_i)\}$, $\theta_i \in \underline{\underline{M}}(G)$ or $\theta_i = 1$ and "Σ" denotes a finite sum.

Proof. The proof is by induction on the length of a word in $\underline{\underline{M}}(G)$. For words of length 1 , the result is given. Let k be a fixed positive integer and suppose that the result is true for all words of length less than or equal to k . Let μ_{k+1} be a word of length $k + 1$. If $\mu_{k+1} = \mu_{k_1} + \mu_{k_2}$, then, since $k_1, k_2 \leq k$, by induction hypothesis μ_{k+1} is of the required kind. If $\mu_{k+1} = \mu_{k_1} . \mu_{k_2}$ then by induction hypothesis $\mu_{k_2} = \Sigma\, \theta_j' \alpha(b_j)$, so that $\mu_{k+1} = \mu_{k_1} \Sigma\, \theta_j' \alpha(b_j) = \Sigma\, \mu_{k_1} \theta_j' \alpha(b_j)$ (by left distributivity) and the inductive step is proved.

A consequence of the proof of the above lemma is the following corollary:

Corollary 3.1.1 Each element of $\underline{\underline{L}}(G)$ has a representation as a word of the form $\Sigma\,\lambda(a_i)$ or $\Sigma\,\theta_i\lambda(a_i)$ where $\theta_i \in \underline{\underline{L}}(G)$

THE ALGEBRAIC SYSTEM $\underline{\underline{L}}(G)$.

We prove the following theorem:

THEOREM 3.2 There exists a group G such that $\underline{\underline{L}}(G)$ is not a sub near-ring of $\underline{\underline{N}}(G)$; and if, for a particular group G , $\underline{\underline{L}}(G)$ is also a sub near-ring of $\underline{\underline{N}}(G)$, then $\underline{\underline{L}}(G) \equiv \underline{\underline{R}}(G)$ * .

Proof. Let G be the infinite dihedral group generated by a and b , b inducing the inverting automorphism on $\{a\}$. The proof consists in showing that $\lambda(b)$ has no additive inverse in $\underline{\underline{L}}(G)$. Let ξ be an arbitrary element of $\underline{\underline{L}}(G)$ and let i be a non-negative integer. If ξ is of length 1 then $a^i\xi = a^i\lambda(a^k) = 1$ or $a^i\xi = a^i\lambda(a^k b) = a^i\lambda(b) = (a^{-i})^b a^i = a^{2i}$; thus ξ maps a^i to a non-negative power of a . Suppose every word in $\underline{\underline{L}}(G)$ of length less than or equal to n maps a^i to a non-negative power of a and let ξ be of length $n + 1$. Then if $\xi = \xi_1 + \xi_2$, then $a^i\xi = a^i\xi_1 . a^i\xi_2$ and by induction hypothesis both $a^i\xi_1$ and $a^i\xi_2$ are non-negative powers of a and hence so is $a^i\xi$. If $\xi = \xi_1 . \xi_2$ then $a^i\xi = (a^i\xi_1)\xi_2 = a^{i'}\xi_2 = a^{i''}$ (by induction hypothesis) where i', i'' are non-negative

---

* We recall that $\underline{\underline{N}}(G)$ is the near-ring of all mappings of G into G .

integers. Thus we have shown that each element of $\underline{\underline{L}}(G)$ maps a^i to a non-negative power of a. Now if ξ is an additive inverse of $\lambda(b)$, then, since $a\xi = a^j$ for some non-negative integer j, we have $1 = a\xi . a\lambda(b) = a^j[b,a] = a^j a^{-b} . a = a^{j+2}$; which is a contradiction since $\{a\}$ is an infinite cycle.

Now suppose for a particular group G that $\underline{\underline{L}}(G)$ is a near-ring. By 1.3.3,

$$\lambda(a) \;=\; \rho(a^{-1}) + \rho(a^{-1})\rho(a) \in \underline{\underline{R}}(G)$$

so that $\underline{\underline{L}}(G) \subseteq \underline{\underline{R}}(G)$. To prove the second part of the theorem it is sufficient to show that $\rho(a) \in \underline{\underline{L}}(G)$ for all $a \in G$. Since $\underline{\underline{L}}(G)$ is a near-ring, there exists an element $\xi_a \in \underline{\underline{L}}(G)$ such that $\xi_a + \lambda(a^{-1})\lambda(a) = 0$. Thus we have

$$\begin{aligned}
\rho(a) &= \lambda(a^{-1}) + \lambda(a^{-1})\rho(a) && \text{(by 1.3.2)} \\
&= \lambda(a^{-1}) + (\xi a + \lambda(a^{-1})\lambda(a)) + \lambda(a^{-1})\rho(a) \\
&= \lambda(a^{-1}) + \xi a + \lambda(a^{-1})(\lambda(a) + \rho(a)) \\
&= \lambda(a^{-1}) + \xi a \in \underline{\underline{L}}(G) .
\end{aligned}$$

Since the choice of a is arbitrary we have the required result.

While a complete characterization of groups for which $\underline{\underline{L}}(G)$ is a near-ring is not known, we prove the following theorem:

THEOREM 3.3 For any group G in the following classes of groups, $\underline{\underline{L}}(G)$ is a sub near-ring of $\underline{\underline{N}}(G)$:

(a) $\underline{\underline{E}}$: The groups all of whose elements are left Engel elements,

(b) $\underline{\underline{D}}$: The groups whose derived groups ~~are periodic~~ have finite exponent n.

Proof. The proof consists in showing that for any group $G \in \underline{\underline{E}} \cup \underline{\underline{D}}$, the elements of $\underline{\underline{L}}(G)$ have their additive inverses in $\underline{\underline{L}}(G)$.

Let $G \in \underline{\underline{E}}$ and let ξ be an arbitrary element of $\underline{\underline{L}}(G)$. By corollary 3.1.1, $\xi = \Sigma_{i=1}^{k} \theta_i \lambda(a_i)$ $(\theta_i \in \underline{\underline{L}}(G)$ or θ_i is a unit element). Since a_i is a left Engel element, there exists an integer m_i such that $\lambda^{m_i}(a_i^{-1}) = 0$ (see page 6). Now, since (by 1.3.2)

$$
\begin{aligned}
\rho(a_i) &= \lambda(a_i^{-1}) + \lambda(a_i^{-1})\rho(a_i) \\
&= \lambda(a_i^{-1}) + \lambda(a_i^{-1})(\lambda(a_i^{-1}) + \lambda(a_i^{-1})\rho(a_i)) \\
&= \ldots = \Sigma_{j=1}^{m_i-1} \lambda^j(a_i^{-1}) + \lambda^{m_i}(a_i^{-1}) + \lambda^{m_i}(a_i^{-1})\rho(a_i) \\
&= \Sigma_{j=1}^{m_j-1} \lambda^j(a_i^{-1}) \quad ,
\end{aligned}
$$

we have

$$
\begin{aligned}
0 &= \lambda(a_i) + \rho(a_i) = \lambda(a_i) + \Sigma_{j=1}^{m_i-1} \lambda^j(a_i^{-1}) \\
&= \theta_i \lambda(a_i) + \theta_i(\Sigma_{j=1}^{m_i-1} \lambda^j(a_i^{-1}))
\end{aligned}
$$

$$= \Sigma_{i=1}^{k} \theta_i \lambda(a_i) + \Sigma_{i=1}^{k} \theta_i (\Sigma_{j=1}^{m_i-1} \lambda^j(a_i^{-1}))$$

$$= \xi + \Sigma_{i=1}^{k} \theta_i (\Sigma_{j=1}^{m_i-1} \lambda^j(a_i^{-1})) \quad .$$

Thus ξ has an additive inverse in $\underline{\underline{L}}(G)$.

Next let $G \in \underline{\underline{D}}$ and let $\xi = \Sigma_{i=1}^{k} \theta_i \lambda(a_i)$ be an arbitrary element of $\underline{\underline{L}}(G)$. Now since

$$0 = n_i \lambda(a_i) = \lambda(a_i) + (n_i - 1)\lambda(a_i)$$

$$= \theta_i \lambda(a_i) + (n_i - 1)\theta_i \lambda(a_i)$$

$$= \Sigma_{i=1}^{k} \theta_i \lambda(a_i) + \Sigma_{i=1}^{k} (n_i - 1)\theta_i \lambda(a_i)$$

$$= \xi + \Sigma_{i=1}^{k} (n_i - 1)\theta_i \lambda(a_i) \quad ,$$

we have the required result.

CRITERION FOR $\underline{\underline{M}}(G)$ TO BE A RING.

We prove the following theorem:

THEOREM 3.4 The commutation near-ring $\underline{\underline{M}}(G)$ is a ring if and only if G is a 3-metabelian group.

Proof. By Lemma 1.5.2, G is 3-metabelian if and only if $\rho(a) + \rho(b) + \lambda(a) + \lambda(b) = 0$ for all $a,b \in G$. Now if $\underline{\underline{M}}(G)$ is a ring then in particular $\rho(b) + \lambda(a) = \lambda(a) + \rho(b)$ and hence

$$\rho(a) + \rho(b) + \lambda(a) + \lambda(b) = \rho(a) + \lambda(a) + \rho(b) + \lambda(b) \underset{\text{(by 1.3.1)}}{=} 0 \quad ;$$

and it follows that G is 3-metabelian. Therefore it remains to prove, conversely, that if $\rho(a) + \rho(b) + \lambda(a) + \lambda(b) = 0$ then $\theta_1 + \theta_2 = \theta_2 + \theta_1$ and $(\theta_1 + \theta_2)\theta_3 = \theta_1\theta_3 + \theta_2\theta_3$ for all $\theta_1, \theta_2, \theta_3 \in \underline{\underline{M}}(G)$. The proof requires the following three lemmas:

<u>Lemma</u> 3.4.1 If G is a 3-metabelian group then in $\underline{\underline{M}}(G)$,

$$P(m,n) : \quad \Pi_{i=1}^{m} \alpha(x_i) + \Pi_{j=1}^{n} \beta(y_j) = \Pi_{j=1}^{n} \beta(y_j) + \Pi_{i=1}^{m} \alpha(x_i)$$

where $\alpha(x_i) \in \{\rho(x_i), \lambda(x_i)\}$, $\beta(y_j) \in \{\rho(y_j), \lambda(y_j)\}$ and m,n are positive integers.

<u>Proof</u>. The proof is by induction on m and n. It follows by an easy application of 1.3.1 that $P(1,1)$ is true. Suppose $P(m,n)$ is true for given m,n. Then replacing y_n in $P(m,n)$ by $y_n\, y_{n+1}$ gives

$$(1) \quad \theta_1 + \theta_2\, \beta(y_n\, y_{n+1}) = \theta_2 \beta(y_n\, y_{n+1}) + \theta_1 ,$$

where $\theta_1 = \Pi_{i=1}^{m} \alpha(x_i)$ and $\theta_2 = \Pi_{j=1}^{n-1} \beta(y_j)$. If in $P(m,n)$, $\beta(y_n) = \rho(y_n)$, then from (1) we get by 1.3.4 and by left distributivity,

$$\theta_1 + \theta_2\rho(y_{n+1}) + \theta_2\rho(y_n) + \theta_2\rho(y_n)\rho(y_{n+1})$$

$$= \theta_2\rho(y_{n+1}) + \theta_2\rho(y_n) + \theta_2\rho(y_n)\rho(y_{n+1}) + \theta_1 ,$$

which by induction hypothesis gives

$$(2) \quad \theta_1 + \theta_2\rho(y_n)\rho(y_{n+1}) = \theta_2\rho(y_n)\rho(y_{n+1}) + \theta_1 .$$

If in $P(m,n)$, $\beta(y_n) = \lambda(y_n)$, then from (1) we get by 1.3.5 and by left distributivity,

$$\theta_1 + \theta_2\lambda(y_n) + \theta_2\lambda(y_n)\rho(y_{n+1}) + \theta_2\lambda(y_{n+1})$$

$$= \theta_2\lambda(y_n) + \theta_2\lambda(y_n)\rho(y_{n+1}) + \theta_2\lambda(y_{n+1}) + \theta_1 ,$$

which again by induction hypothesis gives

$$(3) \quad \theta_1 + \theta_2\lambda(y_n)\rho(y_{n+1}) = \theta_2\lambda(y_n)\rho(y_{n+1}) + \theta_1 .$$

From (2) and (3) we get

$$(4) \quad \theta_1 + \theta_2\beta(y_n)\rho(y_{n+1}) = \theta_2\beta(y_n)\rho(y_{n+1}) + \theta_1 .$$

Now adding $\theta_2\beta(y_n)\lambda(y_{n+1})$ on the right and on the left of both sides of (4), and using left distributivity and 1.3.1 we get

$$(5) \quad \theta_1 + \theta_2\beta(y_n)\lambda(y_{n+1}) = \theta_2\beta(y_n)\lambda(y_{n+1}) + \theta_1 .$$

Now (5) together with (4) gives,

$$(6) \quad \theta_1 + \theta_2\beta(y_n)\beta(y_{n+1}) = \theta_2\beta(y_n)\beta(y_{n+1}) + \theta_1 ,$$

where $\beta(y_{n+1}) \in \{\rho(y_{n+1}),\lambda(y_{n+1})\}$.

Thus we have shown that $P(m,n)$ implies $P(m,n + 1)$ so that by ordinary induction on n it follows that $P(1,n)$ is true for all n and by symmetry $P(m,1)$ is true for all m .

Also for fixed m we have that $P(m,n)$ is true for all n and as m is arbitrary we have proved the lemma.

<u>Lemma</u> 3.4.2 If G is a 3-metabelian group then in $\underline{\underline{M}}(G)$,

$$(\Sigma_{i=1}^{n} \pi_i)\alpha(x) = \Sigma_{i=1}^{n}(\pi_i\alpha(x)) ,$$

where π_i denotes a product in ρ's and λ's and $\alpha(x) \in \{\rho(x),\lambda(x)\}$.

<u>Proof</u>. The proof is by induction on n . If $n = 1$, the result is given. Suppose the result is true for all positive integers less than or equal to a fixed integer n . Then,

$$(\Sigma_{i=1}^{n+1} \pi_i)\alpha(x) = (\Sigma_{i=1}^{n} \pi_i + \pi_{n+1})\alpha(x)$$

$$= \begin{cases} -\pi_{n+1} + (\Sigma_{i=1}^{n} \pi_i)\alpha(x) + \pi_{n+1} + \pi_{n+1}\alpha(x) \\ \qquad \text{(by 1.3.7) if } \alpha(x) = \rho(x) \\ \pi_{n+1}\alpha(x) - \pi_{n+1} + (\Sigma_{i=1}^{n} \pi_i)\alpha(x) + \pi_{n+1} \\ \qquad \text{(by 1.3.8) if } \alpha(x) = \lambda(x) \end{cases}$$

$$= \Sigma_{i=1}^{n} (\pi_i\alpha(x)) + \pi_{n+1}\alpha(x)$$

by induction hypothesis and by lemma 3.4.1

$$= \Sigma_{i=1}^{n+1} \pi_i\alpha(x) .$$

Thus the inductive step is proved.

<u>Lemma</u> 3.4.3 If G is a 3-metabelian group then each element of $\underline{\underline{M}}(G)$ is expressible as a sum of products in ρ's and λ's i.e. if $\mu \in \underline{\underline{M}}(G)$, then

$$\mu = \Sigma_{i=1}^{k} \Pi_{j=1}^{n_i} \alpha(x_{ij}) ,$$

where $\alpha(x_{ij}) \in \{\rho(x_{ij}), \lambda(x_{ij})\}$.

<u>Proof</u>. The proof is by induction on the length of a word in $\underline{\underline{M}}(G)$. For words of length 1, the result is given. Suppose the result is true for all words of length less than or equal to n. Let μ_{n+1} be of length $n+1$. If $\mu_{n+1} = \mu_{n_1} + \mu_{n_2}$ then by induction hypothesis both μ_{n_1} and μ_{n_2} are sums of products in ρ's and λ's and hence μ_{n+1} is of the required form. If $\mu_{n+1} = \mu_{n_1} \cdot \mu_{n_2}$, then by induction hypothesis

$$\mu_{n_1} = \Sigma_{i_1=1}^{k_1} \Pi_{j=1}^{n_{i_1}} \alpha(x_{i_1 j})$$

and

$$\mu_{n_2} = \Sigma_{i_2=1}^{k_2} \Pi_{j=1}^{n_{i_2}} \alpha(y_{i_2 j})$$

so that

$$\mu_{n+1} = \Sigma_{i_2=1}^{k_2} ((\Sigma_{i_1=1}^{k_1} \Pi_{j=1}^{n_{i_1}} \alpha(x_{i_1 j}))\Pi_{j=1}^{n_{i_2}} \alpha(y_{i_2 j}))$$

$$= \Sigma_{i_2=1}^{k_2} \Sigma_{i_1=1}^{k_1} (\Pi_{j=1}^{n_{i_1}} \alpha(x_{i_1 j})\Pi_{j=1}^{n_{i_2}} \alpha(y_{i_2 j}))$$

(by Lemma 3.4.2 used n_{i_2} times) ,

which is again of the required kind and the inductive step is proved.

Now if G is a 3-metabelian group, then by Lemmas 3.4.1 and 3.4.3, it follows that $\theta_1 + \theta_2 = \theta_2 + \theta_1$ for all $\theta_1, \theta_2 \in \underline{\underline{M}}(G)$; and by Lemmas 3.4.1, 3.4.2, 3.4.3 it follows that $(\theta_1 + \theta_2)\theta_3 = \theta_1\theta_3 + \theta_2\theta_3$ for all $\theta_1, \theta_2, \theta_3 \in \underline{\underline{M}}(G)$. Thus the proof of the theorem 3.4 is complete.

<u>CRITERION OF COMMUTATIVITY OF</u> $\underline{\underline{M}}(G)$.

More generally we prove the following theorem:

<u>THEOREM</u> 3.5 The algebraic system $\underline{\underline{R}}(G)(\underline{\underline{L}}(G))$ is commutative if and only if G is nilpotent of class 2.

<u>Proof</u>. If G is nilpotent of class 2 then trivially $0 = \rho(x)\rho(y) = \rho(y)\rho(x)$ and $0 = \lambda(x)\lambda(y) = \lambda(y)\lambda(x)$; and the commutativity of $\underline{\underline{R}}(G)$ and $\underline{\underline{L}}(G)$ follows. Thus it remains to prove, conversely, that each of the identities $\rho(x)\rho(y) = \rho(y)\rho(x)$ and $\lambda(x)\lambda(y) = \lambda(y)\lambda(x)$ imply that G is nilpotent of class 2 . The proof requires the following (more general) lemmas:

Lemma 3.5.1 If z is a 2nd left Engel element of a group G then $z(\pi_1 + \pi_2) = z(\pi_2 + \pi_1)$ where π_1, π_2 are products in ρ's and λ's .

<u>Proof</u>. Since $z\pi_1, z\pi_2$ are contained in the normal closure of z , by Lemma 1.5.4 it follows that $[z\pi_1, z\pi_2] = 1$ and hence the desired result.

Lemma 3.5.2 If z is a 2nd left Engel element of a group G then

(a) if $[z,x,y] = [z,y,x]$ for some $x,y \in G$ then $[x^{-1},y^{-1},z] = 1$;

(b) if $[y,[x,z]] = [x,[y,z]]$ for some $x,y \in G$, then $[x^{-1},y^{-1},z] = 1$.

Proof of (a). We have

$$[z,xy] = [z,y][z,x][z,x,y] = [z,x][z,y][z,y,x]$$
(by Lemma 3.5.1 and by hypothesis)
$$= [z,yx] \; .$$

Thus we have

(7) $\quad [z,xy] = [z,yx]$

Now

$$[z,xy] = [z,[x^{-1},y^{-1}]yx] \qquad \text{by (1.2.1)}$$

$$= [z,yx][z,[x^{-1},y^{-1}]]^{yx}$$

gives $[z,[x^{-1},y^{-1}]] = 1$ so that $[x^{-1},y^{-1},z] = 1$.

Proof of (b). Since $[y,[x,z]] = [x,[y,z]]$ is equivalent to $[x,z,y] = [y,z,x]$, we have

$$[xy,z] = [x,z][x,z,y][y,z] = [y,z][y,z,x][x,z]$$
(by Lemma 3.5.1 and by hypothesis)
$$= [yx,z] \; ,$$

and as before using this we get

$$[xy,z] = [[x^{-1},y^{-1}]yx,z]$$

$$= [x^{-1},y^{-1},z]^{yx}[yx,z]$$

which gives $[x^{-1},y^{-1},z] = 1$. This completes the proof of the lemma.

Now if $\underline{\underline{R}}(G)$ is commutative, we have in particular $[x,y,x] = [x,x,y] = 1$ so that $1 = [y,x,x]^{-[x,y]}$ (by 1.2.6) $= [y,x,x]$. Thus every element is 2nd left Engel in G and by Lemma 3.5.2 (a), G is nilpotent of class 2 .

Similarly if $\underline{\underline{L}}(G)$ is commutative, we have in particular $[x,[y,x]] = [y,[x,x]] = 1$ so that $1 = [y,x,x]$. Thus every element is 2nd left Engel in G and by Lemma 3.5.2 (b) , G is nilpotent of class 2 .

<u>Remark</u>. Let G be a group, such that for a fixed $z \in G$ and all $x,y \in G$ $[z,x,y] = [z,y,x]$ $([y,[x,z]] = [x,[y,z]])$, then replacing y by z it follows that z is 2nd left Engel element in G and by Lemma 3.5.2 it follows that $[z,[x,y]] = 1$, which implies that $[\{z^G\},[x,y]] = 1$, where $\{z^G\}$ is the normal closure of z in G .

Now suppose conversely that for a fixed $z \in G$ and all $x,y \in G$, $[\{z^G\}, [x,y]] = 1$, then from 1.2.10 we have

$$[z,x,y^z][y,z,x^y] = 1 ,$$

which gives in turn

$$[z,x,y[y,z]][y,z,x[x,y]] = 1 \;;$$

$$[z,x,y][y,z,x] = 1 \qquad \text{(since } [z,x],[y,z] \in \{z^G\}) \;;$$

$$[z,x,y] = [x,[y,z]] = [z,y,x]^{[y,z]} \qquad \text{(by 1.2.5)}$$

$$= [z,y,x] \;.$$

Thus we have $[z,x,y] = [z,y,x]$ which also gives

$$[y,[x,z]]^{[z,x]} = [x,[y,z]]^{[z,y]}$$

and hence $[y,[x,z]] = [x,[y,z]]$.

Thus during the course of the proof of Theorem 3.5, Lemma 3.5.2 generalizes a result of LEVIN [17] and it also provides a short proof of his Theorem 2.1 (a) while an easy and short proof of his Theorem 2.1 (b) is contained in the above paragraph.

CHAPTER IV

THE COMMUTATION SEMIGROUPS OF NILPOTENT GROUPS

INTRODUCTION

The main result of this chapter is to prove that the commutation semigroups of nilpotent groups are not in general isomorphic - not even for groups which are both nilpotent and metabelian. This is proved by constructing for every $n \geqq 5$ a metabelian nilpotent group G of class precisely n for which $P(G) \ncong \Lambda(G)$. However we start by proving that these semigroups are identical if the group is nilpotent of class 2 and are isomorphic if it is of class 3. For nilpotent groups of class 4 we prove that the commutation semigroups have the same cardinality.

COMMUTATION SEMIGROUPS OF NILPOTENT GROUPS OF CLASS AT MOST 4

If G is a nilpotent group of class at most n, then $P_1^n = \Lambda_1^n = \{0\}$ where $P_1 = \{\rho(x)\}$ and $\Lambda_1 = \{\lambda(x)\}$. We prove the following theorem.

THEOREM 4.1 Let G be a nilpotent group of class at most 4, then

(a) $P(G) \equiv \Lambda(G)$, if G is of class 2;

(b) $P(G) \cong \Lambda(G)$, if G is of class 3;

and (c) $|P(G)| = |\Lambda(G)|$, if G is of class 4.

Proof. Since $\rho(a) = \rho(b)$ and $\lambda(a^{-1}) = \lambda(b^{-1})$ are both equivalent to $ab^{-1} \in Z(G)$, there is a unique 1 - 1 mapping of P_1 onto Λ_1 which maps $\rho(a)$ to $\lambda(a^{-1})$. Thus

4.1.1 $$|P_1| = |\Lambda_1|$$

Further $\rho(a)\rho(b) = \lambda(a) + \lambda(a)\lambda(b) + \rho(a)$ (by 1.3.6)

$= \lambda(a)\lambda(b)$ (by 1.4.1 and 1.3.1)

gives

4.1.2 $$P_1^2 = \Lambda_1^2 .$$

Also $\rho(a)\rho(b)\rho(c) = \lambda(a^{-1})\lambda(b^{-1})\lambda(c^{-1})$ (by 1.4.4)

gives

4.1.3 $$P_1^3 = \Lambda_1^3 .$$

Now if $\rho(a) = \rho(b)\rho(c)$ then we have

$\rho(b)\rho(c) = \lambda(a^{-1}) + \lambda(a^{-1})\rho(b)\rho(c)$ (by 1.3.2)

$= \lambda(a^{-1}) + \rho(a)\rho(b)\rho(c)$ (by 1.4.4) $= \lambda(a^{-1}) + \rho(b)\rho(c)\rho(b)\rho(c)$

$= \lambda(a^{-1})$, so that $\rho(a) = \rho(b)\rho(c) = \lambda(b)\lambda(c) = \lambda(a^{-1})$.

Thus

4.1.4 $$P_1 \cap P_1^2 = \Lambda_1 \cap \Lambda_1^2$$

And if $\rho(a) = \rho(b)\rho(c)\rho(d)$ then we have

$\rho(b)\rho(c)\rho(d) = \lambda(a^{-1}) + \lambda(a^{-1})\rho(b)\rho(c)\rho(d)$ (by 1.3.2) $= \lambda(a^{-1})$

so that

$$\rho(a) = \rho(b)\rho(c)\rho(d) = \lambda(b^{-1})\lambda(c^{-1})\lambda(d^{-1}) = \lambda(a^{-1}) .$$

Thus

4.1.5 $$\rho_1 \cap \rho_1^3 = \Lambda_1 \cap \Lambda_1^3$$

From (4.1.2) and (4.1.3) we get

4.1.6 $$\rho_1^2 \cap \rho_1^3 = \Lambda_1^2 \cap \Lambda_1^3 .$$

From 4.1.1 to 4.1.6 the proof of the Theorem 4.1 (c) follows immediately. Now if G is nilpotent of class 2, then $\rho(a) = \lambda(a^{-1}) + \lambda(a^{-1})\rho(a)$ (by 1.3.2) $= \lambda(a^{-1})$ gives that $P(G) \equiv \Lambda(G)$. And if G is nilpotent of class 3 then $\rho(a)\rho(b) = \lambda(a^{-1})\lambda(b^{-1})$ (by 1.4.4) $= \rho(a^{-1})\rho(b^{-1})$ (by 4.1.2) $= \lambda(a)\lambda(b)$ (by 1.4.4). Thus the mapping $\rho(a) \longrightarrow \lambda(b^{-1})$ of P_1 onto Λ_1 extends to an isomorphism of $P(G)$ onto $\Lambda(G)$. This completes the proof of the theorem.

COMMUTATION SEMIGROUPS OF NILPOTENT GROUPS OF CLASS $\geqq 5$.

First we prove the following theorem:

THEOREM 4.2 There exists a metabelian nilpotent group G of class precisely 5 whose commutation semigroups are not isomorphic.

Proof.

Construction of G: Let $A = gp\{x_1, x_2, x_3, x_4\}$ be an elementary abelian group of order 5^4. There exist commuting automorphisms α and β of A such that α maps x_1 to x_1x_2, x_2 to x_2x_3, x_3 to x_3x_4 and x_4 to x_4; and β maps

x_1 to x_1x_3 , x_2 to x_2x_4 , x_3 to x_3 and x_4 to x_4 . Both α and β are of order 5 so that we can take two commuting elements a and b of order 5 and form an extension B of A by the cyclic groups $\{a\}$ and $\{b\}$ such that a induces α and b induces β on A . Thus $B = gp\{A,a,b\}$ has the following relations in addition to those of A :

4.2.1 $$a^5 = 1 ; \quad b^5 = 1 ; \quad a^b = a ; \quad x_1^a = x_1x_2;$$
$$x_2^a = x_2x_3; \quad x_3^a = x_3x_4; \quad x_4^a = x_4 ;$$
$$x_1^b = x_1x_3, \quad x_2^b = x_2x_4, \quad x_3^b = x_3 ,$$
$$x_4^b = x_4 .$$

Consider a mapping γ of B into itself mapping x_1 to x_1 ; x_2 to x_2; x_3 to x_3 ; x_4 to x_4 ; a to ax_1^{-1} and b to bx_2^{-1} . Clearly γ is an onto mapping. To show that γ is an automorphism it is sufficient to show that γ preserves the defining relations 4.2.1 of B (see for instance COXETER and MOSER [4], p. 5). We have

$$(a\gamma)^5 = (ax_1^{-1})^5 = a^5x_1^{-5}[x_1^{-1},a]^{10}[x_1^{-1},a,a]^{10}[x_1^{-1},a,a,a]^5 .$$

$$[x_1^{-1},a,a,a,a] = [x_1^{-1},a,a,a,a] = [x_2^{-1}a,a,a] = [x_3^{-1},a,a]$$
$$= [x_4^{-1},a] = 1 \qquad \text{(by 4.2.1)}$$

$$(b\gamma)^5 = (bx_2^{-1})^5 = b^5x_2^{-5}[x_2^{-1},b]^{10}[x_2^{-1},b,b]^{10}[x_2^{-1},b,b,b]^5 \ .$$

$$[x_2^{-1},b,b,b,b] = [x_2^{-1},b,b,b,b] = [x_4^{-1},b,b,b] = 1 \quad \text{(by 4.2.1)}$$

$$(a^b)\gamma = (a\gamma)^{b\gamma} = (ax_1^{-1})^{bx_2^{-1}} = ax_1^{-1}[ax_1^{-1},bx_2^{-1}]$$

$$= ax_1^{-1}[ax_1^{-1},x_2^{-1}][ax_1^{-1},b] = ax_1^{-1}[a,x_2^{-1}][x_1^{-1},b] \quad \text{(by 4.2.1)}$$

$$= ax_1^{-1}.x_2x_3x_2^{-1}.x_1x_3^{-1}x_1^{-1} \quad \text{(by 4.2.1)} = ax_1^{-1} = a\gamma \ .$$

$$(x_i^a)\gamma = (x_i\gamma)^{a\gamma} = x_i^{ax_1^{-1}} = x_i[x_i,ax_1^{-1}] = x_i[x_i,a] \ .$$

So that $(x_i^a)\gamma = x_ix_{i+1} = (x_ix_{i+1})\gamma$ if $i = 1,2,3$ and

$(x_4^a)\gamma = x_4 = x_4\gamma$ (by 4.2.1) .

Finally,

$$(x_i^b)\gamma = (x_i\gamma)^{b\gamma} = x_i^{bx_2^{-1}} = x_i[x_i,bx_2^{-1}] = x_i[x_i,b] \ .$$

So that $(x_i^b)\gamma = x_ix_{i+2} = (x_ix_{i+2})\gamma$ if $i = 1,2$;

$(x_3^b)\gamma = x_3 = x_3\gamma$ and $(x_4^b)\gamma = x_4 = x_4\gamma$.

Thus γ is an automorphism of B and is of order 5 . We take an element c of order 5 and form the splitting extension G of B by the cyclic group $\{c\}$ such that c induces γ on B . Thus $G = gp\{B,c\}$ has the following relations in addition to those of B :

4.2.2 $\quad c^5 = 1$; $\quad x_1^c = x_1$; $\quad x_2^c = x_2$; $\quad x_3^c = x_3$;

$x_4^c = x_4$, $\quad a^c = ax_1^{-1}$, $\quad b^c = bx_2^{-1}$.

The group G we have constructed can be regarded as generated by three elements a , b and c with the following commutator relations:

4.2.3 $$[c,a] = x_1 \;;\quad [c,b] = x_2 \;;\quad [a,b] = 1 \;;$$

$$[c,a,a] = x_2 \;;\quad [c,a,b] = x_3 \;;\quad [c,a,c] = 1 \;;$$

$$[c,b,a] = x_3 \;;\quad [c,b,b] = x_4 \;;\quad [c,b,c] = 1 \;;$$

$$[c,a,a,a] = x_3 \;;\quad [c,a,a,a,a] = x_4 \;;\quad [c,a,b,b] = 1 \;;$$

The following properties of G are immediate :

4.2.4 (a) G is of order 5^7 ;

(b) G is metabelian ;

(c) G is nilpotent of class precisely 5 .

Any element $g \in G$ can be written as :

4.2.5 $$g = a^u b^v c^w z \quad ,$$

Where $u,v,w = 0,1,2,3,4$; and

$$z = x_1^i x_2^j x_3^k x_4^\ell \;,$$

where $i, j, k, \ell = 0, 1, 2, 3, 4$.

<u>Non-isomorphism of $P(G)$ and $\Lambda(G)$</u> :

We shall require the following lemmas,

Lemma 4.2.6 (i) $\rho(x_i)\rho(a) = \rho(x_{i+1})$ for $i = 1,2,3$;

(ii) $\rho(c)\rho(a) = \rho(x_1)$;

(iii) $\rho(a)\rho(a) = \rho(b)$.

Proof of (i)

$$g\rho(x_i)\rho(a) = [g,x_i,a] = [a^u b^v c^w z, x_i, a] \quad \text{(by 4.2.5)}$$

$$= [a^u b^v, x_i, a] \quad (\text{since } c^w z \in C(G')) = [a^u b^v, [x_i, a]] \quad \text{(by 1.2.15)}$$

$$= [a^u b^v, x_{i+1}] \quad \text{(by 4.2.1)} = [a^u b^v c^w z, x_{i+1}] = g\rho(x_{i+1}).$$

Proof of (ii)

$$g\rho(c)\rho(a) = [a^u b^v c^w z, c, a] = [a^u b^v, c, a] = [a^u b^v, [c,a]]$$

$$= [a^u b^v, x_1] = [a^u b^v c^w z, x_1] = g\rho(x_1) .$$

Proof of (iii).

$$g\rho(a)\rho(a) = [g,a,a] = [a^u b^v c^w z, a, a] = [c^w z, a, a]$$

$$= [c^w x_1^i x_2^j x_3^k x_4^\ell, a, a] = [c^w, a, a][x_1^i, a, a][x_2^j, a, a][x_3^k, a, a]$$

$$[x_4^\ell, a, a] \quad \text{(by 1.2.14 (ii))} = [c,a,a]^w [x_1,a,a]^i [x_2,a,a]^j$$

$$[x_3,a,a]^k [x_4,a,a]^\ell \quad \text{(by 1.2.14(i))}$$

$$= [c,b]^w [x_1,b]^i [x_2,b]^j [x_3,b]^k [x_4,b]^\ell \quad \text{(by 4.2.3)}$$

$$= [c^w, b][x_1^i, b][x_2^j, b][x_3^k, b][x_4^\ell, b]$$

$$= [c^w x_1^i x_2^j x_3^k x_4^\ell, b] = g\rho(b) .$$

Since G is metabelian, by Theorem 3.4, $\underline{\underline{M}}(G)$ is a ring of characteristic 5 and in the following lemmas we shall carry out our calculations in $\underline{\underline{M}}(G)$:

Lemma 4.2.7

$$\rho(ac^i x_1^j x_2^k)\rho(a) = \rho(bx_1^i x_2^j x_3^k) ,$$

where $i,j,k = 0,1,2,3,4$.

Proof. We have,

$$\rho(ac^i x_1^j x_2^k)\rho(a)$$

$$= (\rho(a) + \rho(c^i) + \rho(x_1^j) + \rho(x_2^k))\rho(a) \qquad \text{(by 1.3.11)}$$

$$= (\rho(a) + i\rho(c) + j\rho(x_1) + k\rho(x_2))\rho(a) \qquad \text{(by 1.3.10)}$$

$$= \rho^2(a) + i\rho(c)\rho(a) + j\rho(x_1)\rho(a) + k\rho(x_2)\rho(a)$$

$$= \rho(b) + i\rho(x_1) + j\rho(x_2) + k\rho(x_3) \qquad \text{(by Lemma 4.2.6)}$$

$$= \rho(b) + \rho(x_1^i) + \rho(x_2^j) + \rho(x_3^k) \qquad \text{(by 1.3.10)}$$

$$= \rho(bx_1^i x_2^j x_3^k) \qquad \text{(by 1.3.11)}$$

Lemma 4.2.8 $\qquad \rho(ab^2 c^r x_1^s x_2^t)\rho(a^2) = \rho(b^2 x_1^i x_2^j x_3^k)$,

where $i,j,k = 0,1,2,3,4$; $r \equiv 3i \pmod 5$; $s \equiv 3j - 4i \pmod 5$; $t \equiv 3k - 4j + 2i \pmod 5$.

Proof. We have,

$$\rho(ab^2c^rx_1^sx_2^t)\rho(a^2)$$

$$= \quad (\rho(b^2) + \rho(a) + \rho(a)\rho(b^2) + \rho(c^r) + \rho(x_1^s) + \rho(x_2^t))\rho(a^2)$$
(by 1.3.4 and 1.3.11)

$$= \quad (2\rho(b) + \rho^2(b) + \rho(a) + 2\rho(a)\rho(b) + r\rho(c) + s\rho(x_1) + t\rho(x_2))$$
$$(2\rho(a) + \rho(b)) \qquad \text{(by Lemma 4.2.6, 1.3.9, 1.3.10)}$$

$$= \quad 4\rho(b)\rho(a) + 2\rho^2(a) + 4\rho^2(a)\rho(b) + 2r\rho(c)\rho(a) + 2s\rho(x_1)\rho(a)$$

$$+ \quad 2t\rho(x_2)\rho(a) + 2\rho^2(b) + \rho(a)\rho(b) + r\rho(c)\rho(b) + s\rho(x_1)\rho(b)$$

$$+ \quad t\rho(x_2)\rho(b)$$

$$= \quad 5\rho(b)\rho(a) + 2\rho(b) + 6\rho^2(b) + 2r\rho(x_1) + 2s\rho(x_2)$$

$$+ \quad 2t\rho(x_3) + r\rho(x_2) + s\rho(x_3) + t\rho(x_4) \qquad \text{(by Lemma 4.2.6)}$$

$$= \quad 2\rho(b) + \rho^2(b) + 2r\rho(x_1) + (r + 2s)\rho(x_2) + (s + 2t)\rho(x_3)$$
(by characteristic 5 property of $\underline{\underline{M}}(G)$ and since $\rho(x_4) = 0$)

$$= \quad \rho(b^2) + i\rho(x_1) + j\rho(x_2) + k\rho(x_3)$$
(by 1.3.10 and by substituting for r,s,t)

$$= \quad \rho(b^2) + \rho(x_1^i) + \rho(x_2^j) + \rho(x_3^k) \qquad \text{(by 1.3.10)}$$

$$= \quad \rho(b^2x_1^ix_2^jx_3^k) \qquad \text{(by 1.3.11)} .$$

<u>Lemma</u> 4.2.9 $\quad \rho(a^2bc^rx_1^sx_2^t)\rho(a^4) = \rho(b^3x_1^ix_2^jx_3^k)$,

where $i,j,k = 0,1,2,3,4$; $r \equiv 4i \pmod 5$; $s \equiv 4j - i \pmod 5$; $t \equiv 4k - j \pmod 5$.

<u>Proof</u>. We have,

$$\rho(a^2bc^r x_1^s x_2^t)\rho(a^4)$$

$$= (\rho(b) + 2\rho(a) + \rho^2(a) + 2\rho(a)\rho(b) + \rho^2(a)\rho(b) + r\rho(c)$$

$$+ s\rho(x_1) + t\rho(x_2))(4\rho(a) + 6\rho^2(a) + 4\rho^3(a) + \rho^4(a))$$

(by 1.3.4, 1.3.9, 1.3.10, 1.3.11)

$$= 4\rho(b)\rho(a) + 6\rho^2(b) + 8\rho(b) + 12\rho(b)\rho(a) + 8\rho^2(b)$$

$$+ 4\rho(b)\rho(a) + 6\rho^2(b) + 8\rho^2(b) + 4r\rho(c)\rho(a)$$

$$+ 6r\rho(c)\rho^2(a) + 4r\rho(c)\rho^3(a) + 4s\rho(x_1)\rho(a) + 6s\rho(x_1)\rho^2(a)$$
$$+ 4t\rho(x_2)\rho(a)$$

$$= 3\rho^2(b) + 3\rho(b) + 4r\rho(x_1) + 6r\rho(x_2) + 4r\rho(x_3)$$

$$+ 4s\rho(x_2) + 6s\rho(x_3) + 4t\rho(x_3)$$ (since $\underline{\underline{M}}(G)$ is of characteristic 5)

$$= \rho(b^3) + 4r\rho(x_1) + (r + 4s)\rho(x_2) + (4r + s + 4t)\rho(x_3)$$

(by 1.3.10)

$$= \rho(b^3) + i\rho(x_1) + j\rho(x_2) + k\rho(x_3)$$

(by substituting for r,s,t)

$$= \rho(b^3x_1^ix_2^jx_3^k)$$ (by 1.3.10 and 1.3.11) .

<u>Lemma</u> 4.2.10 . $(a^2b^3c^r x_1^s x_2^t)\rho(a^2) = \rho(b^4x_1^ix_2^jx_3^k)$,

where $i,j,k = 0,1,2,3,4$, and r,s,t are as in the Lemma 4.2.8 .

<u>Proof</u>. We have,

$$\rho(a^2b^3c^r x_1^s x_2^t)\rho(a^2)$$

$$= (3\rho(b) + 3\rho^2(b) + 2\rho(a) + \rho^2(a) + 6\rho(b)\rho(a) + 3\rho^2(a)\rho(b)$$

$$+ \quad r\rho(c) + s\rho(x_1) + t\rho(x_2))(2\rho(a) + \rho^2(a))$$

(by 1.3.4, 1.3.9, 1.3.10, 1.3.11)

$$= \quad 6\rho(b)\rho(a) + 3\rho(b)\rho^2(a) + 4\rho^2(a) + 2\rho^3(a) + 2\rho^3(a)$$

$$+ \quad \rho^4(a) + 12\rho(b)\rho^2(a) + 2r\rho(c)\rho(a) + r\rho(c)\rho^2(a)$$

$$+ \quad 2s\rho(x_1)\rho(a) + s\rho(x_1)\rho^2(a) + 2t\rho(x_2)\rho(a) + t\rho(x_2)\rho^2(a)$$

$$= \quad 10\rho(b)\rho(a) + 16\rho^2(b) + 4\rho(b) + 2r\rho(x_1)$$

$$+ \quad r\rho(x_2) + 2s\rho(x_2) + s\rho(x_3) + 2t\rho(x_3) \qquad \text{(by Lemma 4.2.6)}$$

$$= \quad \rho^2(b) + 4\rho(b) + 2r\rho(x_1) + (r + 2s)\rho(x_2) + (s + 2t)\rho(x_3)$$

$$= \quad \rho(b^4) + i\rho(x_1) + j\rho(x_2) + k\rho(x_3) \qquad \text{(by 1.2.10)}$$

$$= \quad \rho(b^4 x_1^i x_2^j x_3^k) \quad . \qquad \text{(by 1.2.11)}$$

Next we prove the following lemma for $\Lambda(G)$:

<u>Lemma</u> 4.2.11. $\lambda(b^2)$ is prime. *

<u>Proof</u>. First we show that $\lambda(b^2) \notin \Lambda_1^2(G)$. Suppose there exist elements $h_1 = a^i b^j c^k z_1$ and $h_2 = a^\ell b^m c^n z_2$ for some $i,j,k, \ell,m,n \in \{0,1,2,3,4\}$ and for some $z_1,z_2 \in G'$ such that

---

* An element of $\rho(G)$ $(\Lambda(G))$ is said to be prime if it can not be expressed as a product of two or more elements of $\rho_1(G)$ $(\Lambda_1(G))$.

$$\lambda(b^2) = \lambda(h_1)\lambda(h_2) .$$

Now since G is metabelian we have from 1.3.6 and 1.3.1 that $\lambda(h_1)\lambda(h_2) = \rho(h_1)\rho(h_2)$ and hence

$$\rho(h_1)\rho(h_2) + \rho(b^2) = 0 ,$$

which gives in turn

$$(\rho(b^j) + \rho(a^i) + \rho(a^i)\rho(b^j) + \rho(c^k z_1))(\rho(b^m) + \rho(a^\ell) + \rho(a^\ell)\rho(b^m)$$

$$+ \rho(c^n z_2)) + \rho(b^2) = 0 \qquad \text{(by 1.3.4 and 1.3.11)} ;$$

$$\mu + (\rho(b^j) + \rho(a^i) + \rho(a^i)\rho(b^j))(\rho(b^m) + \rho(a^\ell) + \rho(a^\ell)\rho(b^m))$$

$$+ \rho(b^2) = 0 \quad (\text{where } \mu = \rho(c^k z_1)\rho(a^\ell b^m)) ;$$

$$\mu + \rho(b^j)\rho(b^m) + \rho(b^j)\rho(a^\ell) + \rho(a^i)\rho(b^m) + \rho(a^i)\rho(a^\ell)$$

$$+ \rho(a^i)\rho(a^\ell)\rho(b^m) + \rho(a^i)\rho(b^j)\rho(a^\ell) + \rho(b^2) = 0 ;$$

$$\mu + mj\rho^2(b) + j\rho(b)(\ell\rho(a) + \frac{\ell(\ell-1)}{2}\rho^2(a))$$

$$+ (i\rho(a) + \frac{i(i-1)}{2}\rho^2(a)).m\rho(b) + (i\rho(a) + \frac{i(i-1)}{2}\rho^2(a)$$

$$+ \frac{i(i-1)(i-2)}{6}\rho^3(a))(\ell\rho(a) + \frac{\ell(\ell-1)}{2}\rho^2(a) + \frac{\ell(\ell-1)(\ell-2)}{6}\rho^3(a))$$

$$+ i\ell m\rho^2(b) + ij\ell\rho^2(b) + 2\rho(b) + \rho^2(b) = 0 \qquad \text{(by 1.3.9)} ;$$

$$\mu + mj\rho^2(b) + j\ell\rho(b)\rho(a) + \frac{j\ell(\ell-1)}{2}\rho^2(b)$$

$$+ mi\rho(a)\rho(b) + \frac{mi(i-1)}{2}\rho^2(b) + \ell i\rho(b) + \frac{\ell i(i-1)}{2}\rho^3(a)$$

$$+ \frac{\ell i(i-1)(i-2)}{6}\rho^2(b) + \frac{i\ell(\ell-1)}{2}\rho^3(a) + \frac{i(i-1)}{2}\frac{\ell(\ell-1)}{2}\rho^2(b)$$

$$+ \frac{i\ell(\ell-1)(\ell-2)}{6}\rho^2(b) + i\ell m\rho^2(b) + ij\ell\rho^2(b) + 2\rho(b) + \rho^2(b)$$

$$= 0 \qquad \text{(by Lemma 4.2.6 (iii))} \ ;$$

$$\mu + (\ell i + 2)\rho^2(a) + (j\ell + mi + \frac{\ell i(i-1)}{2} + \frac{i\ell(\ell-1)}{2})\rho^3(a)$$

$$+ (\frac{i\ell(\ell-1)(\ell-2)}{6} + \frac{\ell i(i-1)(i-2)}{6} + \frac{i(i-1)}{2}\cdot\frac{\ell(\ell-1)}{2} + \frac{j\ell(\ell-1)}{2} + \frac{mi(i-1)}{2}$$

$$+ mj + i\ell m + ij\ell + 1)\rho^4(a) = 0 \quad \text{(by Lemma 4.2.6 (iii))} .$$

Applying c to this last equation and comparing powers of $[c,a,a]$, $[c,a,a,a]$, $[c,a,a,a,a]$ we get

(1) $\ell i + 2 \equiv 0 \pmod 5$

(2) $j\ell + im + \frac{\ell i(i-1)}{2} + \frac{i\ell(\ell-1)}{2} \equiv 0 \pmod 5$

(3) $\frac{i\ell(\ell-1)(\ell-2)}{6} + \frac{\ell i(i-1)(i-2)}{6} + \frac{i(i-1)}{2}\cdot\frac{\ell(\ell-1)}{2}$

$+ \frac{j\ell(\ell-1)}{2} + \frac{mi(i-1)}{2} + mj + i\ell m + ij\ell + 1 \equiv 0 \pmod 5$,

(since $c\mu = 1$) .

From (1) we have either $i\ell = 3$ or $i\ell = 8$.

<u>Case</u> I . ($i\ell = 3$) Let $i = 1$ and $\ell = 3$. Then from (2) we get $3j + m + 3 \equiv 0 \pmod 5$ which gives $m \equiv -(3j + 3) \pmod 5$. Also from (3) we get $1 + 3j + mj + 3m + 3j + 1 \equiv 0 \pmod 5$ so that $mj + j + 3m + 2 \equiv 0 \pmod 5$ which on substituting the value of m gives in turn

$$-j(3j+3) + j - 3(3j+3) + 2 \equiv 0 \pmod 5 \ ;$$

$$-3j^2 - 3j + j - 9j - 9 + 2 \equiv 0 \pmod 5 \ ;$$

$$3j^2 + j + 2 \equiv 0 \pmod 5 \ .$$

But this is not solvable for any integral value of j. (By symmetry we arrive at a similar conclusion by putting $i = 3$ and $\ell = 1$).

Case II. ($i\ell = 8$). Suppose $i = 2$ and $\ell = 4$. Then from (2) we get $4j + 2m + 4 + 12 \equiv 0 \pmod 5$ which is the same as $4j + 2m + 1 \equiv 0 \pmod 5$, so that $m = -(2j + 3) \pmod 5$. Also from (3) we get $8 + 6 + 6j + m + mj + 8m + 8j + 1 \equiv 0 \pmod 5$ so that $4m + 4j + mj \equiv 0 \pmod 5$ which on substituting the value of m gives in turn

$$-4(2j+3) + 4j - j(2j+3) \equiv 0 \pmod 5 \ ;$$

$$-8j - 12 + 4j - 2j^2 - 3j \equiv 0 \pmod 5 \ ;$$

$$-2j - 2j^2 - 2 \equiv 0 \pmod 5 \ ;$$

$j^2 + j + 1 \equiv 0 \pmod 5$. But this again is not solvable for any integral value of j. (By symmetry we arrive at a similar conclusion when $i = 4$ and $\ell = 2$).

Thus we have shown that the existence of $h_1, h_2 \in G$ such that $\lambda(b^2) = \lambda(h_1)\lambda(h_2)$ is impossible and hence $\lambda(b^2) \notin \Lambda_1^2(G)$.

Further $\lambda(b^2) \notin \{\Lambda_1^3(G), \Lambda_1^4(G), \Lambda_1^5(G)\}$ for, if it does, then in particular, we have in turn $\lambda(b^2)\lambda(a)\lambda(a) = 0$;
$\rho(b^2)\rho(a)\lambda(a) = 0$ (since G is metableian) ;
$\rho(b^2)\rho(a)\rho(a) = 0$; $(2\rho(b) + \rho^2(b))\rho(a)\rho(a) = 0$; $2\rho^4(a) = 0$;
$\rho^4(a) = 0$, which is a contradiction since $c\rho^4(a) = x_4 \neq 1$.
This completes the proof of the Lemma 4.2.11.

Now we are in a position to prove the non-isomorphism of $P(G)$ and $\Lambda(G)$.

Let $\overline{P}(G)$ denote the set of all elements $\mu \in P(G)$ such that,

(i) μ is prime

(ii) $\mu^2 \neq 0$

(iii) $\mu^3 = 0$ and

(iv) $\mu P_1^3(G) = 0$;

and let $\overline{\Lambda}(G)$ denote the corresponding set of all elements $\nu \in \Lambda(G)$ such that

(i) ν is prime , (ii) $\nu^2 \neq 0$,

(iii) $\nu^3 = 0$, (iv) $\nu\Lambda_1^3(G) = 0$.

Let $\mu \in P(G)$, then $\mu = \rho(a^i b^j c^k z)$ for some $i,j,k \in \{0,1,2,3,4\}$. Now $\mu P_1^3(G) = 0$ implies in particular ,

$$[c, a^i b^j c^k z, a, a, a] = 1 \quad \text{and} \quad [a, a^i b^j c^k z, a, a, a] = 1$$

which give respectively in turn

$$[c,a^i,a,a,a] = 1 \quad \text{and} \quad [a,c^k,a,a,a] = 1 \;;$$

$$[c,a,a,a,a\;]^i = 1 \quad \text{and} \quad [c,a,a,a,a\;]^k = 1 \;;$$

$$i \equiv 0 \pmod 5 \qquad \text{and} \qquad k \equiv 0 \pmod 5 \;.$$

Thus μ takes the form $\rho(b^j z)$ and by Lemmas 4.2.7 to 4.2.10 it follows that $j \equiv 0 \pmod 5$ for otherwise μ is not prime contrary to our assumption.

But $\mu = \rho(z)$ implies $\mu^2 = \rho^2(z) = 0$, contradictory to our assumption (ii) . Thus it follows that $\bar{P}(G) = \phi$.

On the other hand, by Lemma 4.2.11, $\lambda(b^2)$ is prime; $\lambda^2(b^2) = (2\lambda(b) + \lambda^2(b))(2\lambda(b) + \lambda^2(b)) = 4\lambda^2(b) = 4\rho^2(b)$ $= 4\rho^4(a) \neq 0$; $\lambda^3(b^2) = 0$ and $\lambda(b^2)\Lambda_1^3(G) = 0$, so that $\lambda(b^2) \in \bar{\Lambda}(G)$ and $\bar{\Lambda}(G) \neq \phi$.

But since under any isomorphism of $P(G)$ onto $\Lambda(G)$, $\bar{P}(G)$ maps onto $\bar{\Lambda}(G)$, we conclude that $P(G) \not\cong \Lambda(G)$. This completes the proof of the Theorem 4.2 .

Finally for $n > 5$ we prove the following theorem:

<u>THEOREM</u> 4.3 For each integer $n > 5$, there exists a nilpotent group $\underline{\underline{G}}$ of class n such that $P(\underline{\underline{G}}) \not\cong \Lambda(\underline{\underline{G}})$.

<u>Proof</u>. Let G be the group as constructed in the Theorem 4.2 , and let H be the dihedral group of order 2^{n+1} given as,

$$H = gp\{d,e \mid d^{2^n} = 1 = e^2 \ , \ ede = d^{-1}\} \ .$$

Let $\underline{\underline{G}} = G \times H$ be the direct product of G and H; then we proceed to show that $\underline{\underline{G}}$ is the required group.

Since H is of class n $(n > 5)$, it follows that $\underline{\underline{G}}$ is of class n. Every element of $\underline{\underline{G}}$ can be uniquely written as $a^i b^j c^k z \, e^{\varepsilon} d^{\ell}$ where $i,j,k = 0,1,2,3,4$; $\varepsilon = 0,1$; $\ell = 1,2,\ldots,2^n$ and $z \in G'$.

Let $\bar{P}(\underline{\underline{G}})$ denote the set of all prime elements μ of $P(\underline{\underline{G}})$ such that $\mu^2 \neq 0$, $\mu^3 = 0$ and $\mu P_1^3(\underline{\underline{G}}) = 0$; and let $\bar{\Lambda}(\underline{\underline{G}})$ denote the corresponding set of all prime elements ν of $\Lambda(\underline{\underline{G}})$ such that $\nu^2 \neq 0$, $\nu^3 = 0$ and $\nu\Lambda_1^3(\underline{\underline{G}}) = 0$.

By Theorem 4.2 we already have $\lambda(b^2) \in \bar{\Lambda}(\underline{\underline{G}})$, so that $\bar{\Lambda}(\underline{\underline{G}}) \neq \phi$. Thus it is sufficient to show that $\bar{P}(\underline{\underline{G}}) = \phi$. Let $\mu \in \bar{P}(\underline{\underline{G}})$, then $\mu = \rho(a^i b^j c^k z e^{\varepsilon} d^{\ell})$. Using $\mu P_1^3(\underline{\underline{G}}) = 0$ gives as in Theorem 4.2, that $i \equiv 0 \pmod 5$ $k \equiv 0 \pmod 5$; so that $\mu = \rho(b^j z e^{\varepsilon} d^{\ell})$. Now if $\varepsilon = 1$, then $\mu^3 = 0$ gives in particular,

$$1 = [d, b^j zed^{\ell}, b^j zed^{\ell}, b^j zed^{\ell}]$$

$$= [d,e,e,e] = d^{-2^3} \ ,$$ which is a contradiction,

since $n > 5$. Thus $\varepsilon = 0$ and μ takes the form $\rho(b^j z d^{\ell})$. Further $\mu P_1^3(\underline{\underline{G}}) = 0$ gives, in particular,

$$1 = [e, b^j z d^{\ell}, e,e,e] = [e, d^{\ell}, e,e,e] = d^{-2^4 \ell} \ ,$$

so that $\ell = \pm 2^{n-4}$ or $\ell = 0$. Thus either $\mu = \rho(b^j z d^{\pm 2^{n-4}})$ or $\mu = \rho(b^j z)$. But as in Theorem 4.2, $\mu \neq \rho(b^j z)$; so that $\mu = \rho(b^j z d^{\pm 2^{n-4}})$. Further since

$$\rho(d^{\pm 2^{n-4}}) = \rho(d^{\mp 2^{n-5}})\rho(e) \ ;$$

if $\rho(b^j z) = \rho(g_1)\rho(g_2)$ for some $g_1, g_2 \in G$, then

$$\begin{aligned}
&\rho(g_1 d^{\mp 2^{n-5}})\rho(g_2 e) \\
&= (\rho(g_1) + \rho(d^{\mp 2^{n-5}})) \,.\, (\rho(e) + \rho(g_2)) \\
&= \rho(g_1)\rho(g_2) + \rho(d^{\mp 2^{n-5}})\rho(e) \\
&= \rho(b^j z) + \rho(d^{\pm 2^{n-4}}) \\
&= \rho(b^j z d^{\pm 2^{n-4}}) \ .
\end{aligned}$$

Thus by Lemmas 4.2.7 to 4.2.10 it follows that $j \equiv 0 \pmod 5$, but then $\mu = \rho(zd^{\pm 2^{n-4}})$ implies $\mu^2 = \rho^2(zd^{\pm 2^{n-4}}) = 0$ contrary to our assumption. Thus $\bar{P}(G) = \phi$.

This completes the proof of the Theorem 4.3.

CHAPTER V

SOME GROUP LAWS EQUIVALENT TO THE LAW $[x,y] = 1$

INTRODUCTION

The laws we consider are of the form

$$(*) \qquad [x,y] = C_n ,$$

Where n is an integer greater than 2 and C_n is a left-normad commutator of weight n with entries from the set $\{x,x^{-1},y,y^{-1}\}$. For any group G satisfying $(*)$ we have $\gamma_2(G) = \gamma_3(G)$, so that a nilpotent $*$-group is abelian. First of all we show that a metabelian $*$-group is abelian; and as a consequence we obtain that a soluble (and hence also a finite) $*$-group is abelian. It seems difficult to decide whether or not an arbitrary $*$-group is abelian. While we show that a group satisfying the law $[x,y] = [x,ky^{-1}]$ $(k \geqq 2)$ is abelian, it remains open to prove the same for the law $[x,y] = [x,ky]$ $(k \geqq 4)$. For $k = 2,3$ we are able to prove the equivalence of the law $[x,y] = [x,ky]$ to the law $[x,y] = 1$. Also we exhibit some laws of the form $(*)$ for $n = 3$ and $n = 4$ and show their equivalence to the law $[x,y] = 1$.

SOME GENERAL RESULTS.

First we prove the following theorem:

THEOREM 5.1 A metabelian $*$-group is abelian.

Proof. Let G be a metabelian group satisfying the law $(*)$. Suppose, first, that the 3rd entry in C_n $(n > 2)$ is y or y^{-1}. Then on substituting $[u,v]$ for y the iterated commutator C_n becomes trivial because of the assumed metabelian property hence $[x,y] = [x,[u,v]] = 1$ for all $x \in G$. Thus G is nilpotent of class 2 and hence abelian. If the 3rd entry in C_n is x or x^{-1}, we similarly substitute $[u,v]$ for x and obtain $[x,y] = [u,v,y] = 1$ for all $y \in G$. Thus G is nilpotent of class 2 and hence abelian.

An immediate consequence is the following corollary:

Corollary 5.1.1 A soluble $*$-group is abelian.

Next we prove

THEOREM 5.2 A finite $*$-group is abelian.

Proof. Let G be a minimal counter example. Since the subgroups of G are also $*$-groups, by the minimality of G we have that G is a finite non abelian group all of whose proper subgroups are abelian. Then by well-known Schmidt-Iwasawa Theorem (see for instance IWASAWA [15]) G is soluble and hence abelian by Corollary 5.1.1. Thus no minimal counter example exists and hence all finite $*$-groups are abelian.

Next we prove,

THEOREM 5.3 The following laws in a group are equivalent:

(i) $\quad [x,y] = [x,ky^{-1}] \quad (k \geq 2)$

(ii) $\quad [x,y] = 1$

<u>Proof</u>. Obviously (ii) implies (i) and thus we shall prove that (i) implies (ii) . In (i) on replacing x by $[x,y^{-1}]$ we get

$$[x,y^{-1},y] = [x,y^{-1},ky^{-1}] = [x,(k+1)y^{-1}]$$

$$= [[x,ky^{-1}],y^{-1}] = [x,y,y^{-1}] \qquad (\text{by (i)}) .$$

Thus $[x,y^{-1},y] = [x,y,y^{-1}]$ is a law.

Now we have equivalently

$$[x,y^{-1}]^{-1}[x,y^{-1}]^{y} = [x,y]^{-1}[x,y]^{y^{-1}} \quad ;$$

$$[x,y^{-1}]^{-1}[x,y]^{-1} = [x,y]^{-1}[x,y^{-1}]^{-1} \qquad (\text{by } 1.2.5) \; ;$$

$$[x,y^{-1}]^{-1}[x,y]^{-1}[x,y^{-1}][x,y] = 1 \quad ;$$

$$[[x,y^{-1}],[x,y]] = 1 \quad .$$

Thus by Lemma 1.5.1 every two generated subgroup of a group satisfying the law (i) is metabelian and hence by Theorem 5.1, the group is abelian. Thus (i) implies (ii).

<u>SOME LAWS FOR $n = 3$ AND $n = 4$</u>.

First we prove the following theorem:

<u>THEOREM</u> 5.4 The following law in a group is equivalent to

the commutative law:

(a) $[x,y] = [x,y,y,y]$.

Proof. Changing y to y^{-1} in (a) gives

$$[x,y^{-1}] = [x,y^{-1},y^{-1},y^{-1}] \quad ,$$

which further gives

$$[x,y]^{-y^{-1}} = [[[x,y]^{-y^{-1}},y]^{-y^{-1}},y]^{-y^{-1}} \qquad \text{(by 1.2.5)}$$

$$= [[[x,y]^{-1},y]^{-1},y]^{-y^{-3}} \qquad \text{(by 1.2.4)}$$

$$= [[x,y,y]^{[x,y]^{-1}},y]^{-y^{-3}} \qquad \text{(by 1.2.6)}$$

$$= [x,y,y,y^{[x,y]}]^{-[x,y]^{-1}y^{-3}} \qquad \text{(by 1.2.4)}$$

$$= [x,y,y,y[x,y,y]^{-1}]^{-[x,y]^{-1}y^{-3}} \qquad \text{(by 1.2.2)}$$

$$= [x,y,y,y]^{-[x,y,y]^{-1}[x,y]^{-1}y^{-3}} \qquad \text{(by 1.2.8)}$$

$$= [x,y]^{-[x,y,y]^{-1}[x,y]^{-1}y^{-3}} \qquad \text{(by (a))} .$$

Thus $[x,y]^{y^2[x,y][x,y,y]} = [x,y]$ which gives in turn

$$[[x,y],y^2[x,y][x,y,y]] = 1 \qquad \text{(by 1.2.2)} \quad ;$$

$$[[x,y],y^2[x,y]^y] = 1 \qquad \text{(by 1.2.2)} \quad ;$$

$$[[x,y],y[x,y]y] = 1 \quad ;$$

$$[x,y,y][x,y,y]^{[x,y]y} = 1 \qquad \text{(by 1.2.8)} \quad ;$$

$$[x,y,y][x,y,y]^{y[x,y][x,y,y]} = 1 \qquad \text{(by 1.2.1)} ;$$

$$[x,y,y][x,y,y]^{y[x,y]} = 1 \quad .$$

Thus in particular,

$$[[x,y,y]^{y[x,y]},[x,y,y]] = 1$$

which reduces to ,

$$[[x,y,y][[x,y,y],y[x,y]],[x,y,y]] = 1 \qquad \text{(by 1.2.2)} \quad ;$$

$$[[x,y,y],y[x,y],[x,y,y]] = 1 \qquad \text{(by 1.2.7)} \quad ;$$

$$[y[x,y],[x,y,y],[x,y,y]]^{-[[x,y,y],y[x,y]]} = 1 \quad \text{(by 1.2.6)} \quad ;$$

$$[y[x,y],[x,y,y],[x,y,y]] = 1 \quad ,$$

and hence

$$[y[x,y],[x,y,y],[x,y,y],[x,y,y]] = 1 \quad .$$

This gives by (a), that

$$[y[x,y],[x,y,y]] = 1$$

and equivalently

$$[y[x,y],[y[x,y],y]] = 1 \qquad (\text{since } [x,y,y] = [y[x,y],y] \text{ by 1.2.7}) \quad ;$$

$$[y,y[x,y],y[x,y]]^{[y[x,y],y]} = 1 \qquad \text{(by 1.2.5)} \quad ;$$

$$[y,y[x,y],y[x,y] = 1$$

and hence

$$[y,y[x,y],y[x,y],y[x,y]] = 1 .$$

This gives by (a) , that

$$[y,y[x,y]] = 1 ,$$

so that by 1.2.8 we get

$$[y,[x,y]] = 1 \text{ and in turn}$$

$$[x,y,y] = 1 ;$$

$$[x,y,y,y] = 1 ;$$

$$[x,y] = 1 \qquad \text{(by (a))} .$$

As a consequence of the Theorem 5.4, we get the following corollaries :

Corollary 5.4.1 The following laws are equivalent to the commutative law :

(i) $[x,y] = [x,y^{-1},y^{-1},y]$

(ii) $[x,y] = [x,y,y^{-1},y^{-1}]$

Proof. We have equivalently

$$[x,y] = [x,y^{-1},y^{-1},y] ;$$

$$[x,y^{-1}] = [x,y,y,y^{-1}] ;$$

$$[x,y]^{-y^{-1}} = [x,y,y,y\ ]^{-y^{-1}} \qquad \text{(by 1.2.5)} \ ;$$

$$[x,y] = [x,y,y,y\ ] \ ;$$

$$[x,y] = 1 \qquad \text{(by Theorem 5.4)} \ .$$

Further $[x,y] = [x,y,y^{-1},y^{-1}]$ implies that

$$[x,y,y^{-1},y^{-1}] = [[x,y,y^{-1}],y^{-1},y,y] = [x,y,y,y] \ ;$$

so that we have $[x,y] = [x,y,y,y]$ and hence by Theorem 5.4 , $[x,y] = 1$.

Corollary 5.4.2 The following laws are equivalent to the commutative law :

(i) $[x,y] = [x,y,y]$

(ii) $[x,y] = [x,y^{-1},y]$

(iii) $[x,y] = [x,y,y^{-1}]$

(iv) $[x,y\ ] = [x,y^{-1},y,y^{-1}]$

Proof. Since (i) implies the law $[x,y] = [x,y,y,y]$, by Theorem 5.4, it is sufficient to show that each of the laws (ii), (iii) and (iv) implies (i) .

(ii) implies (i). From (ii) we have in turn,

$$[x,y^{-1}]^{-y} = [x,y^{-1},y^{-1}]^{-y} \qquad \text{(by 1.2.5)} \ ;$$

$$[x,y^{-1}] = [x,y^{-1},y^{-1}] \ ;$$

$$[x,y] = [x,y,y] \quad .$$

(iii) implies (i) From (iii) we have in turn ,

$$[x,y^{-1}] = [x,y^{-1},y] \qquad \text{(replacing } y \text{ by } y^{-1}) \ ;$$

$$[x,y]^{-y^{-1}} = [[x,y]^{-y^{-1}},y] \qquad \text{(by 1.2.5)} \ ;$$

$$[x,y]^{-y^{-1}} = [x,y,y]^{-[x,y]^{-1}y^{-1}} \qquad \text{(by 1.2.6)} \ ;$$

$$[x,y] = [x,y,y]^{[x,y]^{-1}} \quad ;$$

$$[x,y] = [x,y,y]$$

(iv) implies (i) From (iv) we have in turn,

$$[x,y^{-1}] = [x,y,y^{-1},y] \qquad \text{(replacing } y \text{ by } y^{-1}) \ ;$$

$$[x,y]^{-y^{-1}} = [[x,y,y]^{-y^{-1}},y] \qquad \text{(by 1.2.5)} \ ;$$

$$[x,y]^{-y^{-1}} = [[x,y,y]^{-1},y]^{y^{-1}} \qquad \text{(by 1.2.4)} \ ;$$

$$[x,y]^{-y^{-1}} = [x,y,y,y]^{-[x,y,y]^{-1}y^{-1}} \qquad \text{(by 1.2.6)} \ ;$$

$$[x,y] = [x,y,y,y]^{[x,y,y]^{-1}} \quad ;$$

$$[x,y]^{[x,y,y]} = [x,y,y,y] \quad ;$$

$$[x,y,y]^{-1}[x,y][x,y,y] = [x,y,y]^{-1}[x,y,y]^{y} \quad ;$$

$$[x,y]^{y} = [x,y,y]^{y} \quad ;$$

$$[x,y] = [x,y,y] \quad .$$

Next we prove the following theorem,

THEOREM 5.5 The following law in a group is equivalent to the commutative law :

(a) $[x,y]^{y^2} = [x,y,y]$.

Proof. Putting $[x,y] = z$ in (a)* gives

$$z^{y^2} = [z,y] \text{ and equivalently}$$

$$z[z,y^2] = [z,y] \qquad \text{(by 1.2.2)} ,$$

so that

(b) $[y,z] = [y^2,z]z^{-1}$.

Now we have,

$$\begin{aligned}
[y,z]^{z^2} &= [y,z,z] && \text{(by (a))} \\
&= [[y^2,z]z^{-1},z] && \text{(by (b))} \\
&= [y^2,z,z]^{z^{-1}} && \text{(by 1.2.7)} \\
&= ([y^2,z]^{z^2})^{z^{-1}} && \text{(by (a))} \\
&= [y^2,z]^z \\
&= ([y,z]z)^z && \text{(by (b))} \\
&= [y,z]^z z
\end{aligned}$$

---

* This is only an abbreviation.

$$= z[y,z]^{z^2} .$$

So that $z = [x,y] = 1$. This completes the proof of the Theorem 5.5 .

Corollary 5.5.1 The following laws are equivalent to the commutative law :

(i) $[x,y] = [x^{-1},y,x^{-1}]$

(ii) $[x,y] = [x,y,y^{-1},y]$

(iii) $[x,y] = [x,y^{-1},y,y]$

(iv) $[x,y] = [x,y,y,y^{-1}]$

Proof. By Theorem 5.5 it is sufficient to show that each of these laws implies the law $[x,y]^{y^2} = [x,y,y]$.

Interchanging x and y in (i) gives

$$[y,x] = [y^{-1},x,y^{-1}] , \quad \text{which gives that}$$

$$[x,y]^{y^2} = [y^{-1},x,y^{-1}]^{-y^2} = [[x,y]^{y^{-1}},y^{-1}]^{-y^2} \quad \text{(by 1.2.6)}$$

$$= [x,y,y^{-1}]^{-y} = [x,y,y] \quad \text{(by 1.2.5)} .$$

Replacing y by y^{-1} in (ii) gives equivalently $[x,y^{-1}] = [x,y^{-1},y,y^{-1}]$, so that

$$[x,y]^{-y^{-1}} = [x,y^{-1},y,y]^{-y^{-1}} \quad \text{(by 1.2.5)}$$

and hence $[x,y] = [x,y^{-1},y,y]$. Thus the laws (ii) and (iii) are equivalent. Also from (ii), we have,

$$[x,y] = [x,y,y^{-1}]^{-1}[x,y,y^{-1}]^{y}$$

$$= [x,y,y]^{y^{-1}}[x,y,y]^{-1} \qquad \text{(by 1.2.5)} .$$

Thus $[x,y][x,y,y] = [x,y,y]^{y^{-1}}$,

gives $[x,y]^{y} = [x,y,y]^{y^{-1}}$

which gives $[x,y]^{y^2} = [x,y,y]$.

Finally by (iv) we have

$$[[x,y,y],y^{-1}] = [[x,y,y],y^{-1},y^{-1},y]$$

$$= [x,y,y^{-1},y] .$$

Thus $[x,y] = [x,y,y^{-1},y]$ which is (ii) and implies

$[x,y]^{y^2} = [x,y,y]$.

We end this chapter with the following theorem :

THEOREM 5.6. The following laws are equivalent to the commutative law :

(i) $[x,y] = [x,y,x,y]$

(ii) $[x,y] = [x,y^{-1},x,y]$

(iii) $[x,y] = [x,y,y,x]$

Proof. By Lemma 1.5.3, the law $[x,y,y,y] = 1$ implies that the group is 2-metabelian. Thus by Theorem 5.1 it is sufficient to show that each of the laws (i), (ii), (iii) implies the law $[x,y,y,y] = 1$.

Replacing y by xy in (i) gives

$$[x,xy] = [x,xy,x,xy]$$

which gives in turn,

$$[x,y] = [x,y,x,xy] \qquad \text{(by 1.2.8) ;}$$

$$[x,y] = [x,y,x,y][x,y,x,x]^{y} \qquad \text{(by 1.2.8) ;}$$

$$[x,y,x,x] = 1 \qquad \text{by (i) ;}$$

$$[[y,x,x]^{-[x,y]},x] = 1 \qquad \text{(by 1.2.6) ;}$$

$$[[y,x,x]^{-1},x^{[y,x]}] = 1 \qquad \text{(by 1.2.4) ;}$$

$$[y,x,x,x^{[y,x]}]^{-[y,x,x]^{-1}} = 1 \qquad \text{(by 1.2.6) ;}$$

$$[y,x,x,x[y,x,x]^{-1}] = 1 \qquad \text{(by 1.2.2) ;}$$

$$[y,x,x,x]^{[y,x,x]^{-1}} = 1 \qquad \text{(by 1.2.8) ;}$$

$$[y,x,x,x] = 1 \quad .$$

Now (ii) gives equivalently

$$[x,y^{-1}] = [x,y,x,y^{-1}] \qquad \text{(replacing } y \text{ by } y^{-1}\text{) ;}$$

$$[x,y]^{-y^{-1}} = [x,y,x,y]^{-y^{-1}} \qquad \text{(by 1.2.5)} ;$$

$$[x,y] = [x,y,x,y] \quad \text{which is (i)}$$

and hence $[y,x,x,x] = 1$.

Finally replacing x by yx in (iii) gives

$$[yx,y] = [yx,y,y,yx]$$

and hence by 1.2.7

$$[x,y] = [x,y,y,yx]$$

which gives

$$[x,y] = [x,y,y,x][x,y,y,y]^x \qquad \text{(by 1.2.8)} .$$

Thus $[x,y,y,y] = 1$, as required. This completes the proof of the Theorem.

Remark.

As is evident from the contents of this chapter, there is no general method of showing the equivalence of the law $(*)$ to the commutative law. By the techniques used above one could possibly go somewhat further in adding to the list the laws of the type $[x,y] = [u,v,w]$ or $[x,y] = [u,v,w,z]$, where u,v,w,z are elements from the set $\{x,x^{-1},y,y^{-1}\}$. It may be remarked that a non-abelian $*$-group G has $\gamma_2(G) = \gamma_2(\gamma_2(G))$ and that $\gamma_2(G)$ has no proper subgroup of finite index.

CHAPTER VI

ENGEL-LIKE GROUPS

INTRODUCTION.

Let G be a group satisfying the law

$$\text{(a)} \quad x\lambda^{m}(y) = x\lambda^{m+1}(y) .$$

Then we have

$$x\lambda^{m}(y) = y^{-1}(x\lambda^{m}(y))^{-1}y(x\lambda^{m}(y))$$

so that,

$$x\lambda^{m}(y) = 1 \text{ and equivalently } x\rho^{m}(y) = 1 \quad \text{(see page 6)}$$

Thus G is an E_m-group, the group satisfying the mth Engel condition (see page 6).

Corresponding to (a), let G be a group satisfying the law

$$\text{(b)} \quad x\rho^{m}(y) = x\rho^{m+1}(y)$$

$$\text{i.e. } [x,my] = [x,(m + 1)y] ,$$

then we call G an $\underline{\underline{E}}_m$-group. It is readily seen that there is no obvious relation between these two types of groups except that the law (a) implies the law (b). While E_2-groups are nilpotent by LEVI [16] , one has $\underline{\underline{E}}_2$-groups which are not nilpotent (e.g. S_3 , the symmetric group on 3 letters). In this Chapter we prove first of all that an $\underline{\underline{E}}_m$-group without elements of order 3 is an E_m-group (Theorem 6.1); and that every element of odd order is mth left Engel element of the group. While the solubility of $\underline{\underline{E}}_m$-groups in general is not known, we prove: Finite $\underline{\underline{E}}_m$-groups are soluble (Theorem 6.2). A detailed study of $\underline{\underline{E}}_2$-groups is made in [7] and there some properties of $\underline{\underline{E}}_3$-groups are also discussed.

THE MAIN RESULT.

First we prove the following theorem:

THEOREM 6.1. Let G be an $\underline{\underline{E}}_m$-group. If $\gamma_{m+1}(G)$ has no element of order 3, then G is an E_m-group.

Proof. By (b), G satisfies the law

$$[x,my] = [x,(m+1)y] \quad .$$

Hence equivalently

$$6.1.1 \qquad [x,my]^2 = [x,my]^y \quad .$$

Replacing y by y^{-1} and then x by $[x,my]$ in 6.1.1 gives

$$[x,my,my^{-1}]^2 = [x,my,my^{-1}]^{y^{-1}} \quad .$$

This gives in turn,

$$[[x,my,y]^{-y^{-1}},(m-1)y^{-1}]^2 = [[x,my,y]^{-y^{-1}},(m-1)y^{-1}]^{y^{-1}} \quad \text{(by 1.2.5)} ;$$

$$[[x,my]^{-1},(m-1)y^{-1}]^{2y^{-1}} = [[x,my]^{-1},(m-1)y^{-1}]^{y^{-2}} \quad (\text{since } \rho^m(y) = \rho^{m+1}(y)) ;$$

$$[[[x,my]^{-1},y]^{-1},(m-2)y^{-1}]^{2y^{-2}} = [[[x,my]^{-1},y]^{-1},(m-2)y^{-1}]^{y^{-3}}$$

(by 1.2.5 and 1.2.4) ;

$$[[x,my]^{(-1)^2},(m-2)y^{-1}]^{2y^{-2}} = [[x,my]^{(-1)^2},(m-2)y^{-1}]^{y^{-3}}$$

(by 1.2.5 and since $\rho^m(y) = \rho^{m+1}(y)$) .

A repeated application of this process yields

$$[x,my]^{(-1)^m 2y^{-m}} = [x,my]^{(-1)^m y^{-m-1}} ,$$

which gives

$$[x,my]^{2y} = [x,my]$$

and hence by 6.1.1

$$[x,my]^4 = [x,my]$$

which gives

6.1.2 $\quad [x,my]^3 = 1 \quad .$

Thus if $\gamma_{m+1}(G)$ has no element of order 3 , $[x,my] = 1$ and G is an E_m-group. This completes the proof of the Theorem.

From 6.1.2 it follows that an $\underline{\underline{E}}_m$-group satisfies the law $[x,my]^3 = 1$. Thus we have in $\underline{\underline{E}}_m$-groups

$$\begin{aligned}[x,(m-1)y,y^2] &= [x,(m-1)y,y]^2[x,(m-1)y,y,y] \quad \text{(by 1.2.8)} \\ &= [x,my]^2[x,(m+1)y] \\ &= [x,my]^3 \\ &= 1 \qquad \text{(by 6.1.2)}.\end{aligned}$$

Thus if n is an even integer we have in $\underline{\underline{E}}_m$-groups,

$$[x,(m-1)y,y^n] = 1 .$$

Now if $y^k = 1$ where k is an odd integer then $y^{k+1} = y$ and we get

$$1 = [x,(m-1)y,y^{k+1}] = [x,(m-1)y,y] = [x,my] .$$

Thus we have the following Lemma:

Lemma 6.2.1 The odd order elements of an $\underline{\underline{E}}_m$-group are mth left Engel elements.

We use this lemma to prove the following theorem:

THEOREM 6.2 Finite $\underline{\underline{E}}_m$-groups are soluble.

Proof. Let G be a finite $\underline{\underline{E}}_m$-group. By Lemma 6.2.1, all its elements of odd order are mth left Engel in G and hence by Lemma 1.5.5, they lie in $F(G)$, the Fitting radical of G. Thus $G/F(G)$ is a finite 2-group and G, being nilpotent-by-nilpotent, is soluble.

Remark. In [9] we study the groups satisfying the law $x\rho^m(y) = x\rho^{m+n}(y)$ or $x\lambda^{m'}(y) = x\lambda^{m'+n'}(y)$. Every finite group satisfies the above laws for some m, n, m', n'; and in [9] we determine the structure of finite groups in terms of the invariants m, n, m', n'. A typical result is the solubility of a finite group when n or n' is odd. This generalizes Theorem 6.2 above (where $n = 1$).

REFERENCES

[1] Reinhold Baer, "Engelsche Elemente Noetherscher Gruppen", Math. Ann. 133 (1957) 256-270.

[2] D.W. Blackett, "Simple and semisimple near-rings", Proc. Amer. Math. Soc. 4 (1953) 772-785.

[3] R.H. Bruck, "Engel conditions in groups and related questions", (Notes) Third Summer Research Institute of the Austral. Math. Soc. 1963, Canberra.

[4] H.S.M. Coxeter and W.O.J. Moser, "Generators and relations in discrete groups", Springer-Verlag, 1957.

[5] N.D. Gupta, "On commutation semigroups of a group", J. Austral. Math Soc. (to appear).

[6] N.D. Gupta, "Some group laws equivalent to the commutative law", Arch. Math. (to appear).

[7] N.D. Gupta, "Groups with Engel-like conditions", Arch. Math. (to appear).

[8] N.D. Gupta, "Metabelian groups in the variety of certain two-variable laws", Proc. Internat. Conf. Theory of Groups, Austral. Nat. Univ. Canberra, August 1965, Gordon and Breach, New York, 1966 (to appear).

[9] N.D. Gupta and H. Heineken, "Groups with a two-variable commutator identity", (under preparation)

[10] N.D. Gupta and M.F. Newman, "On metabelian groups satisfying certain laws", J. Austral. Math. Soc. (to appear).

[11] Marshall Hall Jr., "The theory of groups" Macmillan, New York 1962.

[12] Hermann Heineken, "Commutator closed groups", Illinois J. Math. 9 (1965) 242-255.

[13] Hermann Heineken, "Engelsche Elemente der Länge drei", Illinois J. Math. 5 (1961) 681-707.

[14] Graham Higman, "Some remarks on varieties of groups", Quart. J. Math. Oxford (2) 10 (1959) 165-178.

[15] K. Iwasawa, " Über die Struktur der endlichen Gruppen, deren echte Untergruppen sämtlich nilpotent sind", Proc. Phys.-Math. Soc. Japan (3) 23 (1941) 1-4.

[16] F.W. Levi, "Groups in which the commutator operation satisfies certain algebraic conditions", J. Indian Math. Soc. (N.S) 6 (1942) 87-97.

[17] Frank Levin, "On some varieties of soluble groups", Math. Zeitschr. 85 (1964) 369-372.

[18] I.D. Macdonald, "On certain varieties of groups", Math. Zeitschr. 76 (1961) 270-282.

[19] B.H. Neumann, "On a conjecture of Hanna Neumann", Proc. Glasgow Math. Assoc. 3 (1956) 13-17.